NOTE TO USERS

This reproduction is the best copy available.

UMI®

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Designing a Secure Ubiquitous Mammography Consultation System

MSc Thesis

By

Lei Yang

Submitted in Partial Fulfillment for the Degree of MSc in Computer Science,
Department of Computer Science,
Lakehead University,

Under the Supervision of Dr. Sabah M. A. MOHAMMED

Thunder Bay, Ontario, CANADA

March 2004

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Library and Archives Canada

Published Heritage Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et Archives Canada

Direction du Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 0-612-96993-2
Our file Notre référence
ISBN: 0-612-96993-2

The author has granted a non-exclusive license allowing the Library and Archives Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou aturement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Abstract

This thesis attempts to design and develop a prototype for mammography image consultation that can work securely within a ubiquitous environment. Mammogram images differ largely from other type of images and it requires special and dedicated techniques to identify the required regions of interest. Thus in Chapter 2 we started to explore the affectivity of the various traditional techniques based on convolution operators (e.g. Sobol, Pretwitt, Canny) for mammography edge detection. The second part of chapter 2 tries to enhance the results obtained via the traditional techniques by hybriding some of them. The hybriding technique is called in our thesis as Pipelined Operators. In this direction we proposed four pipeline operators, which contribute to the edge enhancement as well as abnormalities rendering through the introduction of an additional coloring mechanism. Although the visualization pipelines represent in our view an advancement on the traditional techniques applied to mammograms, such pipelines expose healthcare users to further usage complexities. For this purpose we extended our research work in chapter 2 to find a better single technique that can work smoothly within the healthcare system. In this direction, we developed in the third part of chapter 2 a novel technique for finding edges based on analyzing the dynamic and fuzzy nature of edges in mammograms. We called our developed method as "Dynamic Fuzzy Classifier or the DFC".

In chapter 3, we developed an integral communication infrastructure that can work in a ubiquitous environment like the healthcare system. Three main channels have been identifies as vital for this infrastructure: The healthcare **instant messaging channel** (which we implemented according to W3C recommendation in XML to suite ubiquitous environments), the **image/file transfer channel** (which we implemented via the widely used TCP/IP protocol over the internet), and the **SSL image/file transfer protection protocol**. The combination of these three channels in one simple prototype work fantastically nice when tried by novice healthcare users. It provides simplicity and trust in securing the transferred messages and images/files. The heathcare users need only to plug their ubiquitous device and sends an instant message to their peers and the communication can proceeds afterwards smoothly.

In chapter 4, we introduced further level of security that is highly important for the healthcare system where most of their ubiquitous devices are of the handheld type. It is highly likely that such devices are liable to theft or loss. Hence there is a great need to protect the stored data in such devices using a further security technique. Encryption is the most likely candidate to be used in this direction. However, due the nature of the ubiquitous devices, the use of the well-known heavyweight encryption techniques represents a great performance obstacle. In this direction we been looking to what is generally known as Lightweight encryption technique, which is mostly stream ciphers. For this purpose,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

we implemented most of the notable lightweight stream ciphers used for mobile and ubiquitous environments (e.g. A5, Pless). Moreover, we decided to develop our own lightweight structure just to avoid the possibility of a hacker who may be well aware about the traditional lightweight structures. In this direction we developed a novel lightweight stream cipher that we called the "Dynamic Combiner". The secrecy power of our dynamic combiner is compared to the other traditional lightweight stream ciphers according to the international security standard **FIPS140-1**. The comparison proves our dynamic combiner is far better than the traditional lightweight ciphers. All the comparison experiments performed on mammogram images as well as any other file types.The prototype of our system proves that it can be easily used by healthcare workers for mammography consultation.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Publications and Acknowledgement

A number of publications has been created from this work:

1. *Pakistan Journal of Information & Technology*, Vil.2 No.2, PP178-190, "Morphological Analysis of Mammograms Using Visualization Pipelines". [Mohammed, et.al., 2003(a)] (From Chapter 2)

2. Accepted at the IEEE *Canadian Conference on Computer and Robot Vision* (CRV2004), May 17-19, 2004, University of Western Ontario, Canada, "A Dynamic Fuzzy Classifier for Detecting Abnormalities in Mammograms" [Mohammed, et.al., 2004(a)] (From Chapter 2)

3. *The Asian Journal of Information Technology* Vol.2, No.4, PP. 332-345, 2003, "*Developing an A5 Image Cryptographic System for the 3G GSM Systems Based on Chaotic Image Cryptography*" [Mohammed, et.al., 2003(b)] (From Chapter 4)

4. Accepted at the IEEE 2nd annual conference on Communication Networks and Services (CNSR 2004), Fredericton, N.B., Canada, May 19-21, 2004, "Developing Multitier Lightweight Techniques for Protecting Medical Images within Ubiquitous Environments" [Mohammed, et.al., 2004(b)] (From Chapter 4)

5. Accepted chapter "The Roadmap for Recognizing Regions of Interest in Medical Images" at John Wiley & Sons book entitled "Computer Aided Intelligent Recognition Techniques and Applications" edited by M. Sarfraz to appear in June 2004, [Mohammed, etal., 2004(c)]

I would like to acknowledge the help of Dr. Sabah M.A. Mohammed, my MSc. Thesis supervisor. His knowledge and understanding has helped greatly to make this document what it is.

I would also like to thank Dr. Jinan A.W. Fiaidhi for letting me to work on one of her on going research project on XML [Fiaidhi, et.al., 2004], which helped me to write my XML messenger of chapter 3.

Finally, I would like to thank all faculty members of Computer Science at Lakehead University and my colleagues and fellow MSc. Students for providing such encouraging research environment.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Table of contents

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Chapter 1

Computer-Aided Mammography: Literature Critical Review

1.1 What is Mammography:

Mammograms are complex images which show many variations of both normal and abnormal breast tissue. Screening mammography checks asymptomatic women for signs of breast disease, particularly breast cancer. Diagnostic mammography is used to assess women who have clinical symptoms of breast disease or an abnormality detected on a screening mammogram. As a screening and diagnostic tool, mammography is one of the best ways to detect breast cancer, as mammograms can show cancers that are too small to be felt during physical examination. As the success of breast cancer treatment is improved if a cancer is detected early, using mammography to detect early cancer is very important.

Mammography is a specific type of imaging that uses a low-dose x-ray system for examination of the breasts. The breast is exposed to a small dose of radiation to produce an image of internal breast tissue. The image of the breast is produced as a result of some of the x-rays being absorbed (attenuation) while others pass through the breast to expose either a film (conventional mammography) or digital image receptor (digital mammography). The exposed film is either placed in a developing machine, producing images much like the negatives from a 35mm camera, or images are digitally stored on computer. The images of the breasts can be viewed on film at a view box or as soft copy on a digital mammography workstation (See figure 1).

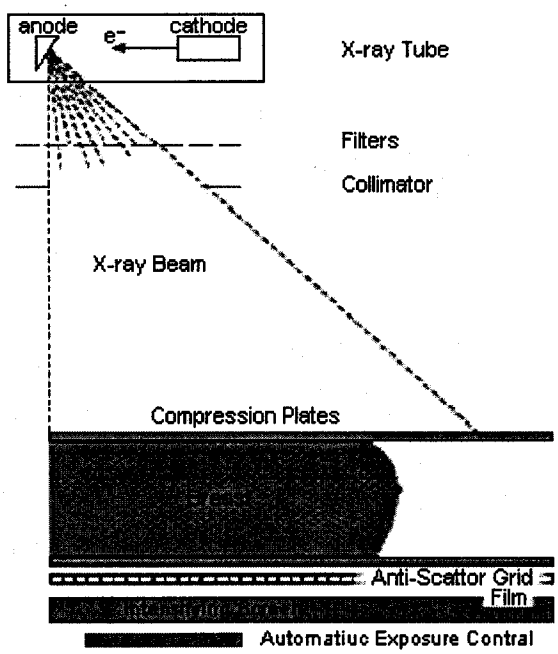


Figure 1.1: Mammography Screening.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Mammograms create black and white images of the breast and the tissue inside the breast. Dense and hard areas appear as white areas on the film, while fattier areas are gray-black in appearance. Tumors, ducts, glands, tiny calcium deposits and benign lumps all show up as thick, white images on a mammogram. A potential tumor or suspicious area has the following criteria. It is an area which 1) is brighter than its surrounding tissue, 2) has uniform density inside the area, 3) has an approximately circular shape of varying size and 4) has fuzzy edges.

The task of mammography interpretation proceeds via a two-step process. In the first step, the object is to detect a solitary geographic area of the breast that will often appear different from other areas of the same and opposing breast. Once an area of the breast can be isolated as being a potential solitary geographic abnormality, the second step involves a determination of whether the morphological features of this area have the appearance of a "normal variation" or benign process. If the solitary geographic abnormality cannot be determined as a "normal variation", then the abnormality is classified as "suspicious" and will require further investigations. Depending on the morphological features of a "suspicious" abnormality, there is a range of probabilities that indicate the likelihood of malignancy.

Most medical experts agree that successful treatment of breast cancer often is linked to early diagnosis. Mammography plays a central part in early detection of breast cancers because it can show changes in the breast up to two years before a patient or physician can feel them.

One of the most recent advances in x-ray mammography is **digital mammography**. Digital (computerized) mammography is similar to standard mammography in that x-rays are used to produce detailed images of the breast. Digital mammography uses essentially the same mammography system as conventional mammography, but the system is equipped with a digital receptor and a computer instead of a film cassette. With digital mammography once the pictures or images have been taken they can be electronically manipulated - the physician can zoom in, magnify, and optimize different parts of breast tissue without having to take an additional image.

1.2 Why Computer-Aided Mammography:

Breast cancer is a major problem for public health in the Western world, where it is the most common cancer among women. In the European Community, for example, breast cancer represents 19% of cancer deaths and fully 24% of all cancer cases. It is diagnosed in a total of 348,000 cases annually in the USA and EC and kills almost 115,000 annually. Approximately 1 in 8 of women will develop breast cancer during the course of their lives,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

and 1 in 28 will die of the disease. There were 900,000 new cases worldwide in 1997 (World Health Organization, 1997). Such grim statistics are now being replicated in Eastern countries as diets and environment become more like their western counterparts.

During the past sixty years, female death rates in the USA from breast cancer stayed remarkably constant while those from almost all other causes declined. The sole exception is lung cancer death rates, which increased sharply from 5 to 26 per 100,000. It is interesting to compare the figures for breast cancer with those from cervical cancer, for which mortality rates declined by 70% after the cervical smear gained widespread acceptance.

The earlier a tumour is detected the better the prognosis. A tumour that is detected when its size is just 0.5cm has a favourable prognosis in about 99% of cases, since it is highly unlikely to have metastasized. Few women can detect a tumour by palpation (breast self-examination) when it is smaller than 1cm, by which time (on average) the tumour will have been in the breast for up to 6-8 years. The 5-year survival rate for localized breast cancer is 97%, this drops to 77% if the cancer has spread by the time of diagnosis and to 22% if distant metastases are found (Journal of the National Cancer Institute 1999).

This is the clear rationale for screening, which is currently based entirely on x-ray mammography (though see below). The UK was the first country to develop a national screening program, though several other countries have established such programs: Sweden, Finland, The Netherlands, Australia, and Ireland; France, Germany and Japan are now following suit. The first national screening program was the UK Breast Screening Program (BSP), which began in 1987. Currently, the BSP invites women between the ages of 50 and 64 for breast screening every three years. If a mammogram displays any suspicious signs, the woman is invited back to an assessment clinic where other views and other imaging modalities are utilized. Currently, 1.3 million women are screened annually in the UK. There are 92 screening centers with 230 radiologists, each radiologist reading on average 5000 cases per year, but some read up to 20,000.

The restriction of the BSP to women aged 50 and above stems from fact that the breasts of pre-menopausal women, particularly younger women, are composed primarily of milk-bearing tissue which is calcium-rich; this milk-bearing tissue involutes to fat during the menopause – and fat is transparent to x-rays. So, while a mammogram of a young woman appears like a white-out, the first signs of tumours can often be spotted in those of post-menopause women. In essence, the BSP defines the menopause to be substantially complete by age 50!

The UK program resulted from the Government's acceptance of the report of the committee chaired by Sir Patrick Forrest. The report was quite bullish about the effects of a screening

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

program. To date, the BSP has screened more than eleven million women and has detected over 65,000 cancers. Research published in the BMJ in September 2000 demonstrated that the NHS Breast Screening Program is saving at least 300 lives per year. The figure is set to rise to 1,250 by 2010. More precisely, Moss (British Medical Journal 16/9/2000), demonstrated that the National Health Service breast screening program, begun in 1987, resulted in substantial reductions in mortality from breast cancer by 1998. In 1998, mortality was reduced by an average of 14.9% in those aged 50 to 54 and 75 to 79, which would be attributed to treatment improvements. In the age groups also affected by screening (55 to 69), the reduction in mortality was 21.3%. Hence, the estimated direct contribution from screening was 6.4%.

Recent studies suggest that the rate of interval cancers that appear between successive screening rounds is turning out to be considerably larger than predicted in the Forrest Report. Increasingly, there are calls for mammograms to be taken every two years and for both a cranio-caudal and mediolateral oblique image to be taken of each breast.

Currently, some 26 million women are screened in the USA annually (approximately 55 million worldwide). In the USA there are 10,000 mammography-accredited units [13]. Of these, 39% are community and/or public hospitals, 26% are private radiology practices, and 13% are private hospitals. Though there are 10,000 mammography centres, there are only 2,500 mammography specific radiologists – there is a worldwide shortage of radiologists and radiologic technologists (the term in the UK is radiographers). Huge numbers of mammograms are still read by non-specialists, contravening recommended practice, nevertheless continuing with average throughput rates between 5 and 100 per hour. Whereas expert radiologists have cancer detection rates of 76-84%, generalists have rates which vary from between 8-98% (with varying numbers of false-positives). The number of cancers that are deemed to be visible in retrospect, that is, when the outcome is known, approaches 70% (American Journal of Roentgenology 1993). Staff shortages in mammography seem to stem from the perception that it is "boring but risky": as we noted earlier, 12% of all malpractice lawsuits in the United States are against radiologists, with the failure to diagnose breast cancer becoming one of the leading reasons for malpractice litigation (AJR 1997 and Clark 1992) The shortage of radiologists is driving the development of specialist centers and technologies (computers) that aspire to replicate their skills. Screening environments are ideally suited to computers, as they are repetitive and require objective measurements.

As we have noted, screening has already produced encouraging results. However, there is much room for improvement. For example, it is estimated that a staggering 25% of cancers are missed at screening. It has been demonstrated empirically that double reading greatly improves screening results; but this is too expensive and in any case there are too few screening radiologists. Indeed, recall rates drop by 15% when using 2 views of each breast.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Double reading of screening mammograms has been shown to half the number of cancers missed. However, a study at Yale of board (British Medical Journal, 1999) certified, radiologists showed that they disagreed 25% of the times about whether a biopsy was warranted and 19% of the time in assigning patients to 1 of 5 diagnostic categories. Recently, it has been demonstrated that single screening plus the use of computer-aided diagnosis (CAD) tools – image analysis algorithms that aim to detect microcalcifications and small tumours – also greatly improve screening effectiveness, perhaps by as much as 20%.

Post-screening, the patient may be assessed by other modalities such as palpation, ultrasound and increasingly, by MRI. 5-10% of those screened have these extended "work-up". Post work-up, around 5% of patients have a biopsy. In light of the number of tumours that are missed at screening (which reflects the complexity of diagnosing the disease from a mammogram), it is not surprising that clinicians err on the side of caution and order a large number of biopsies. In the US, for example, there are over one million biopsies performed each year: a staggering 80% of these reveal benign (non-cancerous) disease.

It has been reported that between screenings 22% of previously taken mammograms are unavailable or are difficult to find, mostly due to the fact that they have been misfiled in large film archives – lost films are a daily headache for radiologists around the world, 50% were obtained only after major effort, Bassett et al. (American Journal of Roetentology, 1997).

1.3 Approaches to Computer-Aided Mammography:

The early detection of breast cancer is most reliably achieved with mammography. However, 10% to 30% of women who have breast cancer and who undergo mammography have negative mammograms [Holland, 1982]. In approximately two thirds of these false negative mammograms the radiologist failed to detect the cancer that was evident retrospectively [Guillemet, 1996]. It is difficult for the human radiologist to maintain interest in interpreting large numbers of images in which only a small number show abnormalities. Hence the need to construct computer-aided systems to diagnose breast cancer in mammograms becomes apparent. Computerized schemes are being developed for the specific detection of either mass lesions or microcalcifications. Some of the significant methods are described as follows:

Local area grey level thresholding [Davies, Dance, 1992]:
Using this method the mean and standard deviation are determined within a square kernel centred at the pixel of interest to estimate the local background fluctuations. If the pixel in question has a value larger than the mean pixel value multiplied by a preselected multiple of the standard deviation then it is retained, otherwise it is set to a constant value. A modal filter is then used to produce a uniform background level

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

outside the breast.

Global grey level thresholding [Giger, 1993]:
With global thresholding a preselected percentage of pixels with values at the high end of the grey-level histogram are retained and all others are set to a constant value.

Box-rim filtering:
The box rim filter usually consists of a 9x9 template with a central 3x3 box matched to the individual microcalcification and outermost rim with 2 pixel width to consider surrounding background. This process is developed to enhance object to background contrast in the image with highest values corresponding to the location of potential microcalcification. A global thresholding is then applied to the filtered image such that the pixels with grey scale value among the top 5% of the histogram are preserved. The 5% threshold value is chosen such that all true microcalcifications are included in the resultant image.

Median filtering:
Median filtering has been found to be very powerful in removing noise from 2-d signals without blurring edges [Bovik AC, 1987]. This makes it particularly suitable for enhancing images. To apply median filtering to a digital picture, we replace the value at a pixel by the median of the values in a neighbourhood of the pixel. Two dimensional median filters can be defined for arbitrary sizes and shapes of filter windows W(i,j), such as line segments, squares, circles and crosses. The 2-dimensional median filtering operation is defined as follows. For a 2-d filter window W(i,j) centred at image coordinates (i,j) of a picture $\{x_{ij} : (i,j) \in Z^2\}$, the median filtering output is x_{ij} = median $\{x_{rs} : (r,s) \in N(i,j)\}$ $(i,j) \in Z^2$ where N(i,j) is the area in the image covered by window W(i,j). Median filters have several properties which make them superior to low pass filters [Kuhlmann F, 1981]. If an image has impulse like noise, median filtering can remove it without significantly distorting the signal, and if an image contains edges, median filtering can preserve them due to the fact that only a small fraction of the neighbourhood overlaps with the edge.

Selective median filtering:
The edge preservation power of the standard median filter is not sufficient for enhancing mammogram images due to the fuzziness of the boundaries of suspicious areas. A modification of the filter, selective median filter (SMF), was defined by Lai et al [Lai S, 1989]. For a window W(i,j) centred at image coordinates (i,j) the output of the selective median filter is x_{ij} = median $\{x_{rs} : (r,s) \in N(i,j)$ and $| x_{rs} - x_{ij} | < T\}$ where $(i,j) \in Z^2$, N(i,j) is the area in the image covered by window W(i,j) and T is a threshold. In computing the median, the set of pixels is restricted to those with a difference in grey

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

level no greater than some threshold T. By adjusting the parameter T, the amount of edge smearing can be controlled. If T is small, the edge preserving power of SMF is strong but it's smoothing effect will be small. If T is large, the SMF behaves the other way around. This modification of the median filter is related to selective averaging schemes developed for linear filters [Rosenfeld R, 1982] that show good results in improving the edge preserving power of linear low pass filters. To achieve strong noise suppression, one can either use a filter with a large window size or the filter can be applied repeatedly. The first approach has several drawbacks [Nodes TA, 1982]. The median filter, designed to act as a low pass filter in homogenous areas, will respond more and more like a bandpass filter as window size is increased. Further, increasing the window size leads to increased noise suppression, but also to increased signal distortion. On the other hand, they showed iterated median filtering reduces an original signal to an invariant signal, called root signal, and that only piecewise constant images are roots to the median filters, implying that edge information is not lost by iterating the filtering process. In general SMF could be described as a "nearest neighbour" median filter.

Comparing left and right breasts:

At the University of Chicago, Geiger and colleagues [Yin FF, 1993] have developed a scheme for the detection of masses on mammograms. This scheme is based on the architectural symmetry of normal right and left breasts with asymmetries indicating potential masses. After automatic recognition of corresponding left and right breasts a non-linear subtraction technique is used in which grey-level thresholding is performed on the individual mammogram prior to subtraction. Ten thresholded images with different cut-off grey levels are obtained from the right and left breast images. Next, subtraction of the corresponding left and right breast images is performed to generate 10 bilateral subtraction images. The data in these images are linked and the information from the 10 subtracted images is accumulated into two images which contain enhanced contrast of suspected masses for both breasts.

Texture analysis:

Texture analysis was used by Undrill et al [Undrill P, 1996] at the University of Aberdeen to detect suspicious masses in mammography. Textural features of an image contain information about the spatial distribution of tonal variations. The concept of tone is based on the intensity of pixels within a defined region. The texture of a region describes the pattern of spatial variation of tonal values in a neighbourhood which is small compared to the region. The method used is based on Laws matrices. These are 5 labelled vectors which are combined to form matrices.

When convolved with a textured image these matrices extract individual structural components of the image. The RR mask was found to give the best results. This mask

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

is an iso-directional, differentiating filter giving a relatively uniform response in smooth areas such as breast masses compared with more highly textured regions such as adipose tissue. So that these regions can be thresholded, a derived image is generated by calculating the variance over a small window centred about each point in the texture image. This is a measure of texture energy. Median smoothing was then applied to the texture energy images, to reinforce the difference between zones of micro structure detected by the masks by reducing the effects of noise and local variability within dissimilar regions. Thresholding is the simplest method of segmentation using intensity values to classify image domain into objects and background. Two thresholding stages were needed since the texture masks extract not only the relatively smooth regions of the masses but also the smooth film background. The first stage, applied to the texture energy image, segmented it into smooth and highly textured regions, by applying upper and lower thresholds. From a definition of texture energy homogenous regions have higher values. A threshold was taken from a histogram of smoothed texture energy which contained a lower peak representing the highly textured regions and an upper peak representing the smoothly textured region. Secondly, a segmentation refinement was applied using a logical mask derived from the co-incidence of areas of near-zero intensity values of the equalized original image and texture energy threshold to eliminate the uniform dark film background. This threshold level could be set at a fixed value across all the images. The final result of the segmentation process was a binary image of lesion segmentation objects against a non-lesion background. This filter and image processing sequence was able to produce outlines of both regular masses and stellate lesions which were well matched to those of an expert, though the technique was unable to distinguish between the two lesion types.

Investigating the Laplacian transform of an image:

The technique used by Highnam [Hingham, et.al., 1996] for the detection of masses uses a pre-processing step which involves segmentation of the mass and transformation of the original mammographic images to the "h-int representation" [Hingham R.P, 1996]. A circumscribed mass is pictured as a hill in the h-int representation and any "halo" is a moat. The detection of the existence and extent of any halo is the purpose of the algorithm. Mathematically, going from a mass to the surrounding area might correspond to a change in the curvature of the h-int surface perpendicular and this suggests using the sign of the Laplacian of h-int to determine the edge of the mass and the moat. Since it appears likely that any halo will be equal over the mass we can look at the sign of the average Laplacian, and this aids numerical stability. The results of this method indicate that genuine masses (both benign and malignant) exhibit a negative Laplacian, whilst the surrounding tissue always exhibits a positive Laplacian. This suggests that there is some kind of halo around every mass. The halo seems to be some kind of covering of the mass, probably equal in thickness all-round. This cover appears to deform with the mass so that benign masses have

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

widely varying halo extents, whereas solid masses have fixed extent. This in turn suggests that compression is having a large effect on the benign masses and so some measure of compressibility based upon the mass shape itself might well allow differentiation of benign and malignant masses.

Fuzzy logic:

In Richmond, Canada, Sameti and Ward developed an algorithm to detect masses which is based on the theory of fuzzy sets [Sameti M, 1996]. The algorithm is intended to be a part of a soft tissue abnormality detection scheme. The algorithm divides a mammogram into different regions according to its intensity information. For those mammograms which contain a lesion with brighter intensity than other patterns present in the mammogram, the algorithm can successfully detect the borders of the lesion. Design of the algorithm is based on 2 main properties of mammographic lesions and patterns. Firstly, because of the unclear boundaries of the parenchyma and malignant masses in a mammogram, employing the principles of fuzzy sets in assigning the image pixels to different regions is appropriate. Secondly, since abnormal tissue lesions and masses are usually larger than a certain size, in determining which segmented region a pixel belongs to, the effects of its neighbouring pixels as well as its own intensity value must be considered. The algorithm divides the image into 2 regions by completion of the following steps, see figure 1.1:

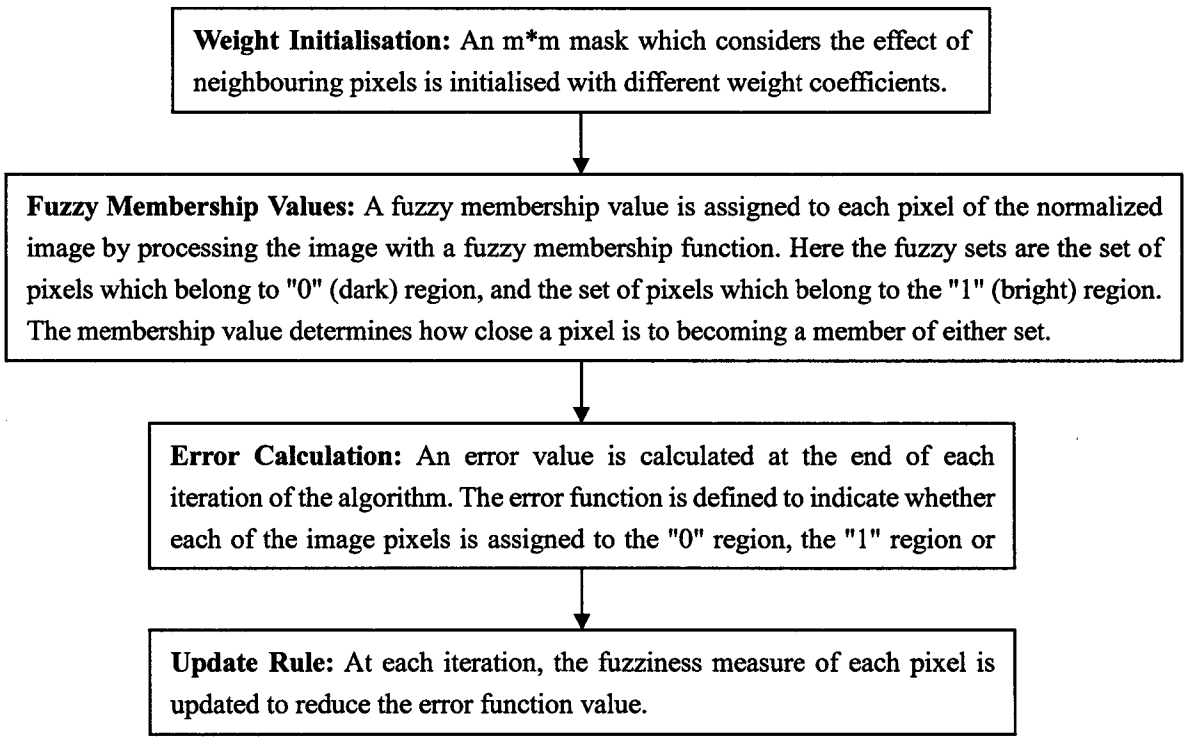


Figure 1.1: Fuzzy logic masses detection algorithm

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

The algorithm with four desired levels of segmentation was implemented and applied on a set of 20 mammographic images, each containing a malignant mass, and the algorithm was successful in segmenting each image into four regions. It also successfully detected the boundaries of those masses, appearing brighter than other regions in each of the mammograms.

Fractal texture model:

Given the size of mammographic film and the fine sampling that is needed to detect microcalcifications, the amount of data to be dealt with is quite large. Guillemet et al [Guillemet H, 1996] designed this method for the automatic detection of microcalcifications which reduces step by step the amount of data. At each step the reduction is achieved by rejecting some parts of the image in which clusters are likely to lie. The steps used are as Figure 1.2 illustrates:

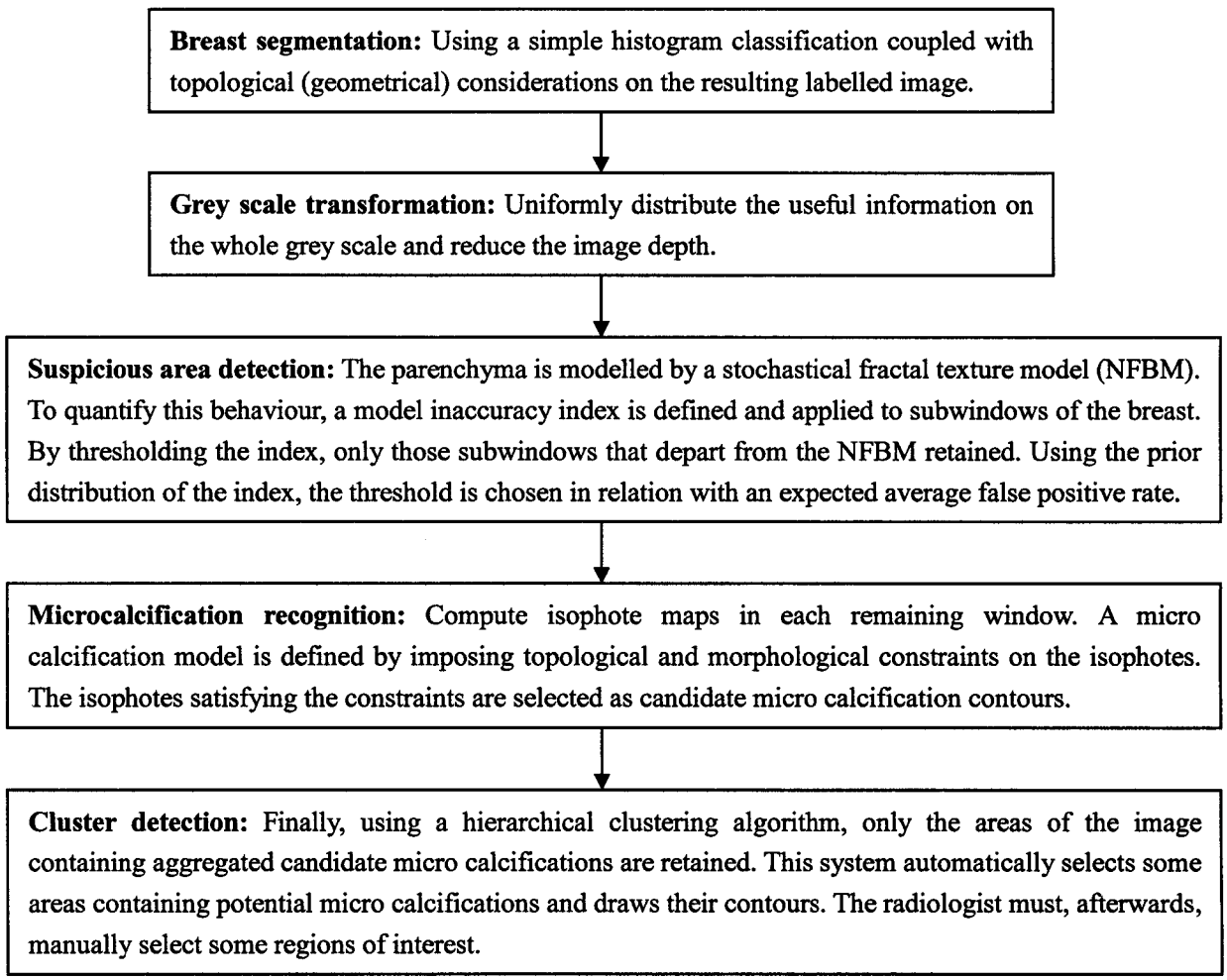


Figure 1.2: Fractal texture model

A space scale approach:

In the space scale approach developed in Bremen University by Thomas Netsch [Netsch,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

1996], the image is preprocessed using a Laplacian of Gaussian (LoG) filter. This acts as a multiscale spot detector but because the LoG can be regarded as a band pass filter too many structures in the mammogram are regarded as possible calcifications.Therefore, a mathematical model of a micro calcification is introduced to enhance detection. The model describes the micro calcification as a circular, bright spot of a certain diameter D and local contrast C. A cylindrical or 2D gaussian shaped model are possible choices. The model is only said to be a micro calcification if the contrast C exceeds a predefined threshold. This threshold depends on the diameter D in the model and is used to set up a certain level of detection sensitivity in the performance evaluation. It is shown that the model has a characteristic response in the space scale depending on its parameters D and C. This response can be thought of as a reference for the response of a probable location of a micro calcification. Given a bright spot marked by the LoG detection the corresponding parameters of the model are estimated from its response. If the estimated contrast is greater than the predefined threshold, the spot is reported as a micro calcification otherwise it is not. Due to the gaussian, blurring spots are occasionally not marked at their exact centre which degrades the correlation model. Therefore, candidates on coarser scales are located at smaller scales by tracking the local extreme in the spacescale - a technique which is well known in space scale theory. This method is highly sensitive to the detection of individual micro calcifications. In order to reduce the number of false positives a simple clustering system is used to locate groups of calcifications.

Wavelet techniques:

Research into the detection of micro calcifications using the wavelet transform has been carried out in Leeds by McLeod et al [McLeod, et.al., 1996]. This technique was designed to replace the FFT (fast fourier transform) method as it was found to be simpler and more efficient. Extraction of possible microcalcifications is firstly achieved by wavelet decomposition of the mammogram using Deubechies wavelets to 3 levels. Investigations showed that the 8th order was the maximum trade off between the cleanest presentation of the microcalcification signal and the obscurity due to ringing effects. This research also showed that microcalcifications are mostly prominent in the highpass subbands of levels 2 and 3, with level 1 containing mostly noise and fine structural detail. The transform was applied across the image as a sequence of 512 x 512 pixel regions, which are overlapped to allow the removal of edge artefacts. The reconstructed image can be post-processed by convolution with a matching spatial filter. This reduces the strength of the remaining structural information, while retaining the signal from the icrocalcifications. A global threshold is applied based on image statistics to remove remaining background information and binarise the image. Finally an isolated pixel delete operation removes the majority of solitary one pixel size objects. Cluster evaluation is performed using a method which examines local statistics in a $1cm^2$ (302 pixel) region centred around each object in the thresholded image. The

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

object is removed if the statistics fall below a predetermined value, and is retained otherwise, indicating the object is a member of a cluster of 3 or more objects within the $1cm^2$ area (convention for a micro-calcification cluster). This method is less demanding than using particle-counting algorithms while still providing good discrimination of clusters based on the above criteria. Research shows that wavelets can be very effective in detecting micro-calcification type of cancer.

Mathematical morphology methods:

In Recife, Brazil, Mendonca Braga Neto et al [Mendonca, et.al., 1996] have developed a method which uses the Watershed method in the segmentation of calcifications in images. The Watershed method is a powerful mathematical morphology tool for segmentation (which does not involve heuristics (investigations)). The watershed transformation may be viewed as a flooding of the image interpreted as relief. The watershed lines are the closed contours that divide the image into several adjacent basins. Since the gradient operator has the property of enhancing grey-level transitions, the watershed line of the gradient gives theoretically a good segmentation operator. In practise due to noise and the low contrast of mammograms, a regularisation of the gradient is required to eliminate basins which are not genuine. The regularisation of the gradient, is accomplished by imposing markers as the regional minima of the gradient and then suppressing all the other minima by way of a morphological reconstruction operation. Hence, one must provide internal markers, one for each calcification and also a background or external marker. The markers were obtained in a semi-automatic way. The internal markers were single pixels placed manually inside each calcification with a mouse. The external markers were obtained from the internal markers as a result of the watershed transformation of the inverse of the input mammographic section using the internal markers as the marker set. Research has shown that the watershed method is very effective for the automatic detection of microcalcifications. Despite the poor contrast of mammographic images and the presence of overlapping calcifications, satisfactory results were obtained. Better results are expected by counting on the assistance of an experienced radiologist.

Neural networks:

In an effort to detect individual microcalcifications, neural networks are most commonly applied to regions containing clusters of microcalcifications. A more effective technique has been developed by Meersman, Scheunders and Van Dyke [Meersman, et.al., 1996] at the University of Antwerp in Belgium which uses neural networks to perform a pixel based classification. The networks used were three-layered feedforward neural networks with varying dimensions. The neighbourhood of each pixel (9x9 or 15x15 pixels) within the image was given as input to the network, the output of the statistical method was considered as the correct output. The networks had a hidden layer of 16 or 81 units and one output unit and were trained using the backpropogation algorithm. The regions selected for evaluation were processed by the network and the resulting

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

images were analysed for the presence of detected clusters by the following method:

- First, a threshold was applied on the result images. A group of connected pixels having a value above the threshold value were regarded as a calcification.
- Next, all calcifications containing only a single pixel were removed because they are considered as noise.
- In a third step, all pixels within 0.5cm of the calcification region were marked. A marked region containing 2 (or more) calcifications was considered as a detected cluster. After comparison of the location and size of the detected clusters and the true clusters, the detected clusters were either classified as true positive (TP) or false positive (FP) clusters. By changing the threshold value the amount of TP and FP clusters found was changed.

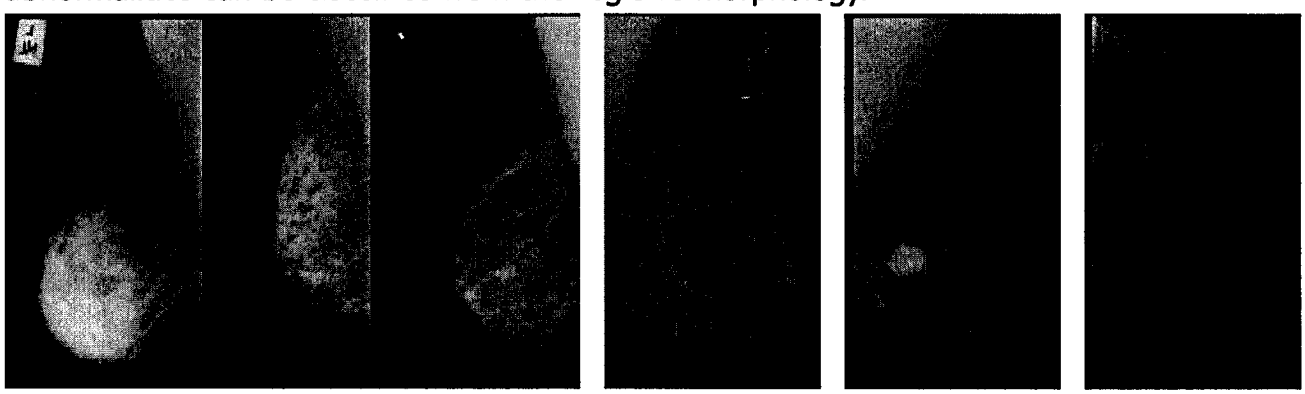
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Chapter 2

Diagnosing Abnormalities in Mammograms Based on Edge Detection

2.1 Introduction

Searching for the presence of abnormalities in mammographic data is an important step in the detection and diagnosis of breast cancer and other breast illnesses. There are many abnormal shapes that we may encounter when analyzing mammograms. Some of these abnormalities represent harmless regions such as Lipoma (.e. fatty regions) and Hylanizing Fibroadenomas(i.e. dense fiber area). However, other abnormalities such as stellate lesions, Circumscribed masses and Calcification clusters may represent suspected cases of breast cancer. Figure 2.1 illustrates these different breast abnormalities. All such breast abnormalities can be classified from the region's morphology.



Lipoma Fibroadenomas Normal Calicification Circumscribed Stellate

Figure 2.1: Different Abnormalities within mammograms.

2.2 Traditional Morphological Analysis Techniques

When research into image processing of mammograms began, the preprocessing step was the only enhancement carried out on the image. In more recent years an extra step has been added to most enhancement methods which has led to more accurate shape detection of early tumors. The additional steps includes wide image processing techniques based on Convolution, Thresholding, and Mathematical Morphology. In this section we examine their basic effects on breast abnormalities visualization.

2.2.1 Convolution Operators

Convolution is a mathematical operation that is fundamental to many common image processing processes. Convolution provides a mechanism for edge detection through 'multiplying together' two arrays of numbers to produce a third array of numbers of the same dimensionality. This can be used in image processing to implement operators whose output pixel values are simple linear combinations of certain input pixel values. In an image-processing context, one of the input arrays is normally a image. The second array is

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

usually much smaller, and is also two-dimensional, and is known as the kernel. Figure 2.2 shows an example image and kernel that we will use to illustrate convolution.

I_{00}	I_{01}	I_{02}	I_{03}	I_{04}	I_{05}	I_{06}	I_{07}	I_{08}
I_{10}	I_{11}	I_{12}	I_{13}	I_{14}	I_{15}	I_{16}	I_{17}	I_{18}
I_{20}	I_{21}	I_{22}	I_{23}	I_{24}	I_{25}	I_{26}	I_{27}	I_{28}
I_{30}	I_{31}	I_{32}	I_{33}	I_{34}	I_{35}	I_{36}	I_{37}	I_{38}
I_{40}	I_{41}	I_{42}	I_{43}	I_{44}	I_{45}	I_{46}	I_{47}	I_{48}
I_{50}	I_{51}	I_{52}	I_{53}	I_{54}	I_{55}	I_{56}	I_{57}	I_{58}
I_{60}	I_{61}	I_{62}	I_{63}	I_{64}	I_{65}	I_{66}	I_{67}	I_{68}
I_{70}	I_{71}	I_{72}	I_{73}	I_{74}	I_{75}	I_{76}	I_{77}	I_{78}

K_{00}	K_{01}	K_{02}
K_{10}	K_{11}	K_{12}
K_{20}	K_{21}	K_{22}

Figure 2.2: Convolution Process requires an Image and a Kernel.

The convolution is performed by sliding the kernel over the image, generally starting at the top left corner, so as to move the kernel through all the positions where the kernel fits entirely within the boundaries of the image. Each kernel position corresponds to a single output pixel, the value of which is calculated by multiplying together the kernel value and the underlying image pixel value for each of the cells in the kernel, and then adding all these numbers together [Batchelor 1993]. Figure 2.3 illustrates this operation. Using convolution the value of the output pixel O_{22} can be calculated as follows:

$$O_{22}=I_{11}*K_{00}+I_{12}*K_{01}+I_{13}*K_{02}+I_{21}*K_{10}+I_{22}*K_{11}+I_{23}*K_{12}+I_{32}*K_{20}+I_{32}*K_{21}+I_{33}*K_{22}$$

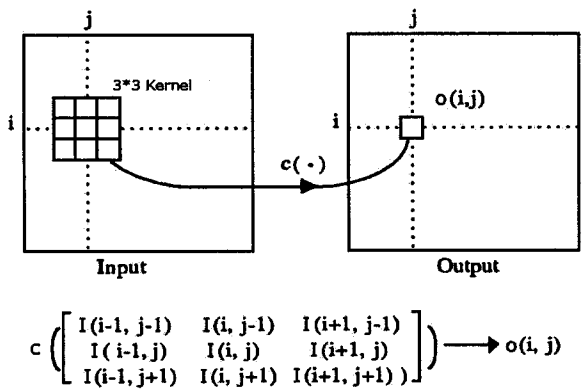


Figure 2.3: Illustrating the Process of Convolution.

The convolution process is a highly researched issue and it is affected by many factors. Basic to all is the kernel type being used and the size of the kernel. There are many types of kernels had been proposed in the literature [Gonzalez & Woods 2002] and basic to all are the following kernel types:

- The **Roberts Cross**: Operator performs a simple, quick to compute, 2-D spatial gradient measurement on an image. The operator consists of a pair of 2×2 convolution kernels. One kernel is the other rotated by 90°.

G_x | 1 | 0 |
|---|---|
| 0 | -1 |

G_y | 0 | 1 |
|---|---|
| -1 | 0 |

$$|G|=|G_x|+|G_y|$$

These kernels are designed to respond maximally to edges running at 45° to the pixel grid, one kernel for each of the two perpendicular orientations. We can see that the result image is very dark when applying the Roberts Cross operator to mammogram.

- **Laplacian**: Is a 2-D isotropic measure of the 2nd spatial derivative of an image. The Laplacian of an image highlights regions of rapid intensity change and is therefore often used for edge detection.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

-1	-1	-1
-1	8	-1
-1	-1	-1

And

-1	-4	-1
-4	20	-4
-1	-4	-1

- **Sobel**: Operator performs a 2-D spatial gradient measurement on an image and so emphasizes regions of high spatial frequency that correspond to edges. Typically it is used to find the approximate absolute gradient magnitude at each point in an input image. Sobel Kernels are:

-1	0	1
-2	0	2
-1	0	1

And

-1	-2	-1
0	0	0
1	2	1

These kernels are designed to respond maximally to edges running vertically and horizontally relative to the pixel grid, one kernel for each of the two perpendicular orientations. The kernels can be applied separately to the input image, to produce separate measurements of the gradient component in each orientation (call these G_x and G_y). These can then be combined together to find the absolute magnitude of the gradient at each point $|G| = \sqrt{G_x^2 - G_y^2}$ and the orientation of that gradient. An approximate magnitude can be computed using: $|G| = |G_x| + |G_y|$.

- **Compass**: Edge Detection is an alternative approach to the differential gradient edge detection. When using compass edge detection the image is convoluted with a set of (in general 8) convolution kernels, each of which is sensitive to edges in a different orientation. For each pixel the local edge gradient magnitude is estimated with the maximum response of all 8 kernels at this pixel location: $|G| = \max(|Gi| : i = 1 \text{ to } n)$ where G_i is the response of the kernel i at the particular pixel position and n is the number of convolution kernels. The local edge orientation is estimated with the orientation of the kernel that yields the maximum response. Various kernels can be used for this purpose; and best of all are the Prewitt and the Kirsch kernels. Two templates out of the set of 8 are shown below:

0^0:

-1	1	1
-1	-2	1
-1	1	1

45^0:

1	1	1
-1	-2	1
-1	-2	1

- **Kirsch** Edge Detector [Parker 1997] is another compass kernel. The masks given by these templates try to model the kind of grey level change seen near an edge having various orientations. There is a mask for each of eight compass directions. For instance K0 implies a vertical edge (horizontal gradient) at the pixel corresponding at the center of the mask. To find the edge, I is convolved with the eight masks at each pixel position. The response is the maximum of the responses of any of the eight masks and the directions quantified into eight possibilities.

K0:

-3	-3	5
-3	0	5
-3	-3	5

K1:

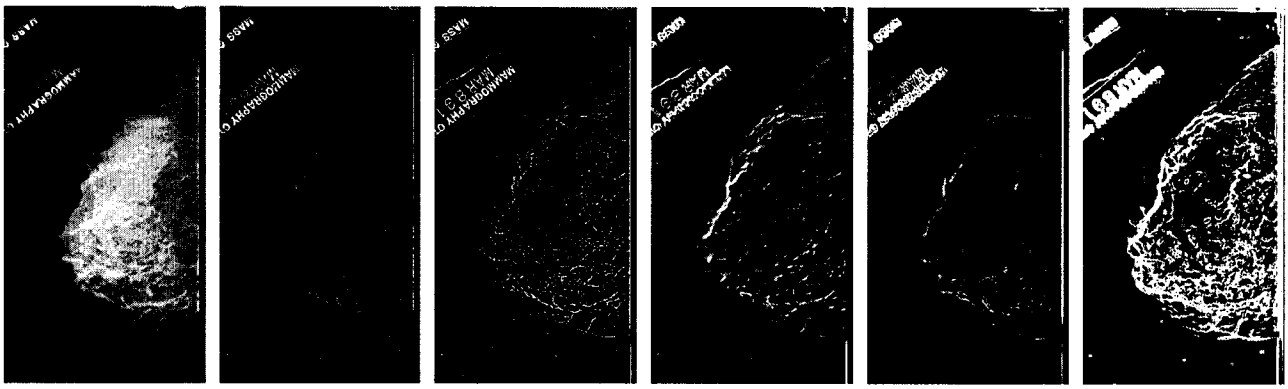
-3	5	5
-3	0	5
-3	-3	-3

... ...

The effects of using these kernels on mammogram's tumor detection vary so much as figure 2.4 illustrates. The experiment shows that Kirsch and Sobel kernels have better

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

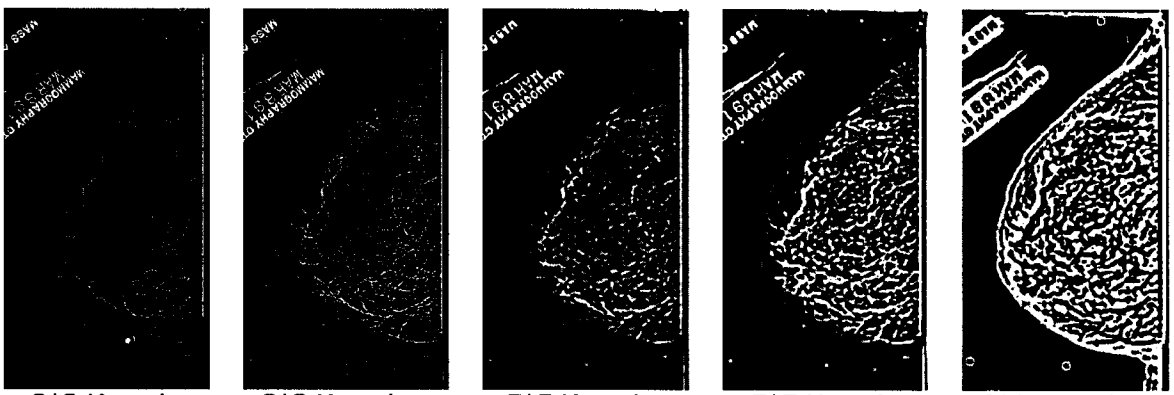
detection power from the other kernels.



Original Image Roberts Cross Laplacian Sobel Prewitt Compass Kirsch Compass

Figure 2.4: The effects of different kernel types on breast tumor's detection.

Kernel size can affect the resolution power of the convolution processes. It can increase the thickness of the edge detected. Figure 2.5 illustrate the results of another experiment conducted using the Laplacian Kernel and varying its size from 3x3 to 9x9. That is why most of the researchers use 3x3 or 5x5 kernel size avoiding over or under resolution.



3*3 Kernel 3*3 Kernel 5*5 Kernel 7*7 Kernel 9*9 Kernel

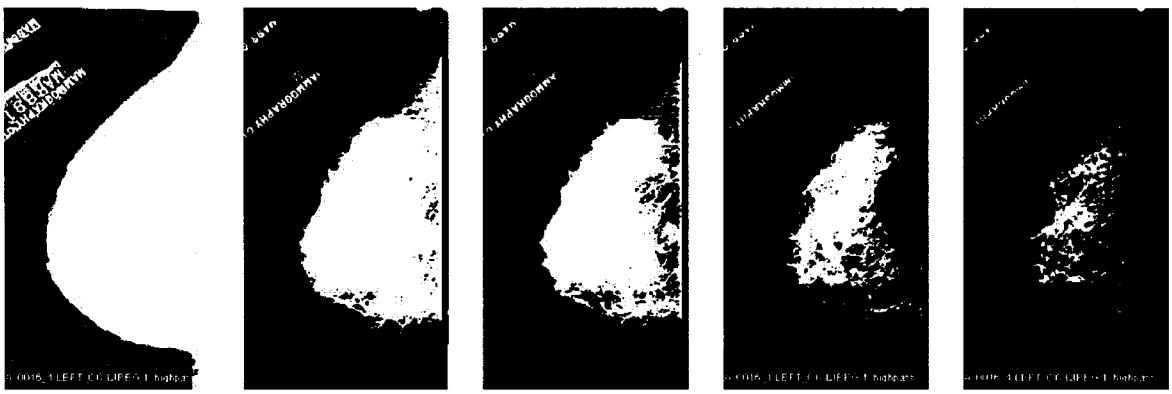
Figure 2.5: Effects of the Kernel Size on the Convolution Resolution.

2.2.2 Thresholding Operators

Threshold makes color changes across a programmer-determined "boundary", or threshold, more obvious. This technique uses a specified threshold value, minimum value, and maximum value to control the color component values for each pixel of an image. Color values below the threshold are assigned the minimum value. Values above the threshold are assigned the maximum value. The threshold process is performed for each color component of each pixel. When the operation is complete, the color components of the destination image pixels will contain either the minimum value or the maximum value. For example, consider what happens to an image when a threshold operation is performed with a minimum of 0 and a maximum of 255. After the image is processed, the red, green, and blue values of the pixels will be either 0 or 255. In the following examples, we write threshold value in (min, threshold, max) format. We can see that the white area (indicate

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

the higher brightness area) getting smaller with the threshold value go up. Thresholding is a very important morphological technique for detecting tumor regions because a tumor represent a dense tissue area of the breast structure. However, it very tricky to find the right threshold value that can work for variety of mammograms. For this purpose many researchers tried to arrive at a dynamic threshold which can learn its optimal value from the type of image under analysis. Figure 2.6 illustrates the effects of using various of static thresholds.



(0, 18, 255) (0,138,255) (0, 160, 255) (0, 216, 255) (0, 240, 255)

Figure 2.6: Effects of various static thresholds.

2.2.3 Mathematical Morphology Operators

Morphological operators often take a binary image and a structuring element as input and combine them using a set operator (intersection, union, inclusion, complement). For the basic morphological operators the structuring element contains only foreground pixels (i.e. ones) and `don't care's'. These operators, which are all a combination of erosion and dilation, are often used to select or suppress features of a certain shape, e.g. removing noise from images, skeletonization-thinning or selecting objects with a particular direction. Morphological operators can also be applied to gray-level images, e.g. to reduce noise or to brighten the image. The method is to treat the image as a sequence of binary images by operating on each gray level as if it were the 1 value and assuming everything else to be 0. The resulting images can then be combined by laying them on top of each other and "promoting" each pixel to the highest gray-level value coincident with that location. Mathematical morphology provides a number of important image processing operations, including erosion, dilation, opening and closing.

Erosion: The basic effect of the operator on a binary image is to erode away the boundaries of regions of foreground pixels (i.e. white pixels, typically). Thus areas of foreground pixels shrink in size, and holes within those areas become larger. To compute the erosion of a binary input image by this structuring element, we consider each of the foreground pixels in the input image in turn. For each foreground pixel (which we will call the input pixel) we superimpose the structuring element on top of the input image so that the origin of the structuring element coincides with the input pixel coordinates. If for every pixel in the structuring element, the corresponding pixel

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

in the image underneath is a foreground pixel, then the input pixel is left as it is. If any of the corresponding pixels in the image are background however, the input pixel is also set to background value.

Dilation: The basic effect of Dilation operator on a binary image is to gradually enlarge the boundaries of regions of foreground pixels. Thus areas of foreground pixels grow in size while holes within those regions become smaller.

Opening and **closing** are both derived from the fundamental operations of erosion and dilation. The basic effect of an opening is like erosion in that it tends to remove some of the foreground (bright) pixels from the edges of regions of foreground pixels. However it is less destructive than erosion in general. As with other morphological operators, the exact operation is determined by a structuring element. The effect of the operator is to preserve foreground regions that have a similar shape to this structuring element, or that can completely contain the structuring element, while eliminating all other regions of foreground pixels. Closing is similar in some ways to dilation in that it tends to enlarge the boundaries of foreground (bright) regions in an image (and shrink background color holes in such regions), but it is less destructive of the original boundary shape. Figure 2.7 illustrates the effects of applying repetitive erosion and dilation operators on mammograms.

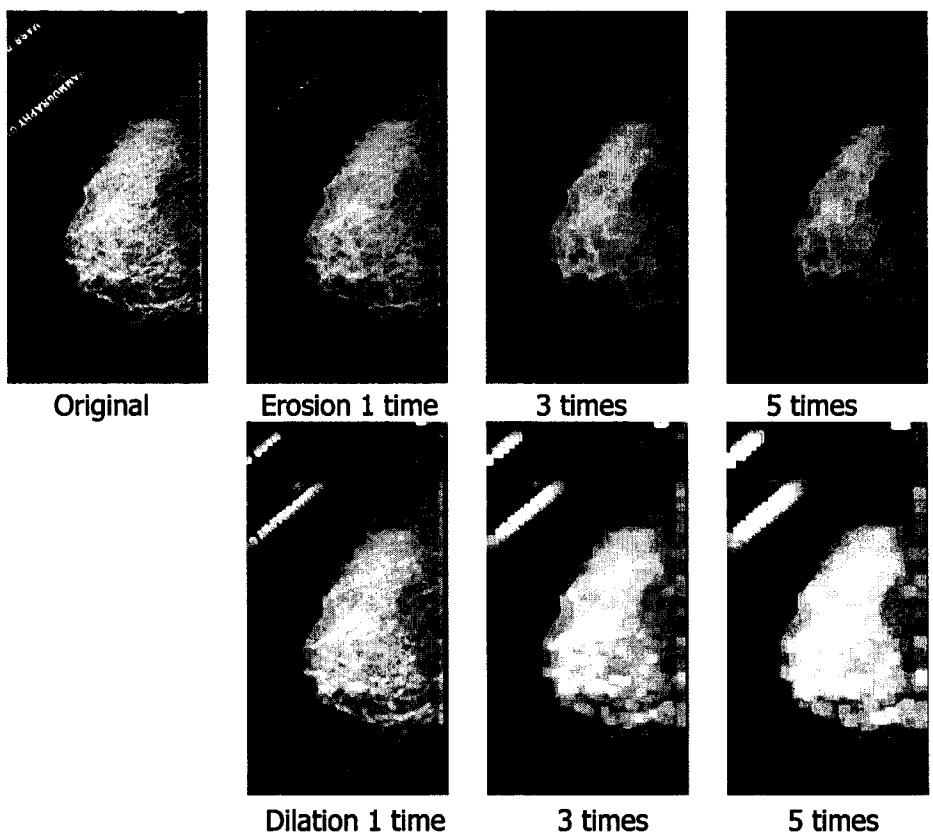


Figure 2.7: The effects of Applying three times the Erosion and Dilation Operators.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

It is obvious that erosion aims at thinning the region while dilations reduce the noise within the image regions. opening and closing operations have no obvious effects on the mammograms. The structuring element used in these experiments is 3x3 matrix with all elements equal to 1.

2. 3 Visualization Pipelines:

Usually research in volume visualization [Elvins 1992] is used to create images from scalar and vector datasets defined on multiple dimensional grids, i.e., it is the process of projecting a multidimensional (usually 3D) dataset onto a 2D image stack to gain an understanding of the structure contained within the data. After the image stack is processed by 2-D image processing techniques, it can then be reconstructed into either a 3-D volumetric dataset or a rendered 2D image. This is a new but rapidly growing field in both computer graphics and data visualization [Bredlie & Wood 2001]. These techniques are used in medicine, geoscience, astrophysics, chemistry, microscopy, mechanical engineering, and other areas. Visualization is usually achieved using either volume or surface rendering techniques.

- ***Volume rendering*** is a computer graphics technique whereby the object or phenomenon of interest is sampled or subdivided into many cubic building blocks, called volume elements. Each volume element can be treated separately. The resulted volume elements can be assembled from multiple 2-D images (i.e. image stack), and are displayed by projecting these images into either 2-D pixel space or storing them as frames for 3D projection.
- In ***surface rendering***, the volumetric data must first be converted into geometric primitives, by a process such as isosurfacing, isocontouring, surface extraction or border following. These primitives (such as polygon meshes or contours) are then rendered for display using conventional geometric rendering techniques.

Both techniques have advantages and pitfalls. A major advantage of the volume rendering technique is that the image data volume can be displayed without any knowledge of the geometry of the dataset and hence without intermediate conversion to a surface representation. This conversion step in surface rendering can sometimes be quite complex, especially if surfaces are not well defined (i.e. noisy 2-D images) and can require a lot of user intervention (such as manual contour tracing.)

In this section we are proposing certain pipelines for mammograms volume visualization. Such visualization pipelines are based on the proper choice of various morphological transfer operators in order to map the original image data into meaningful optical properties of the volume to be visualized. The transfer operators represents basic segmentation methods (e.g convolution, thresholding) as well as other binary operators such as add, subtract, invert, overlay, erosion, and dilation.

The visualization pipelines can be simple when the rendered image is composed of using only binary operations such as erosion and inversion (see Figure 2.8).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

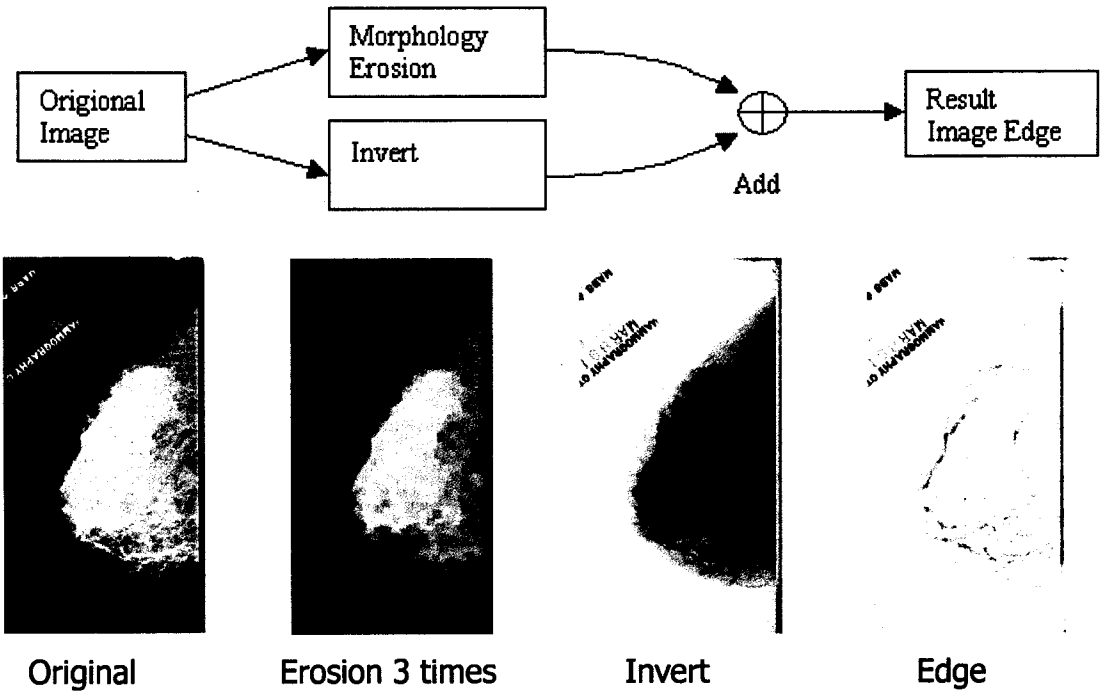


Figure 2.8: Simple Visualization Pipleline.

More complex visualization pipelines can be produced when edge detection operators are involved. Figure 9 illustrates our first expirement when the we used a thresholding value of (210) to segment the image into high brightness and low brightness areas.

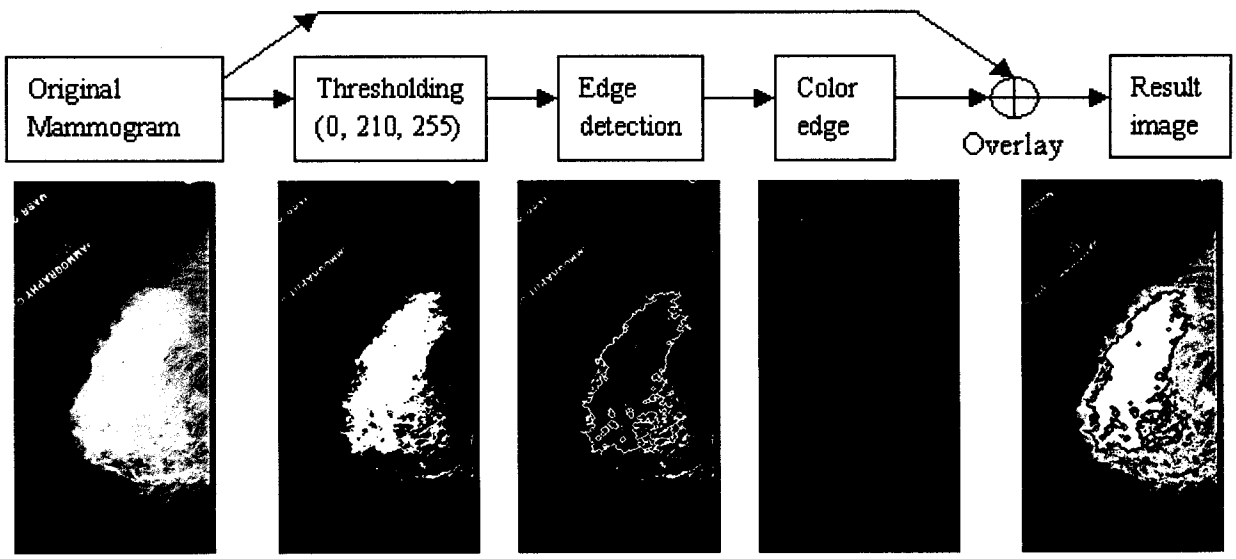


Figure 2.9: Visualization Pipeline aiming at separating the image into high and low brightness areas

We can use more than one threshold value to highlight the various volume elements in the image as Figure 2.10 illustrates:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

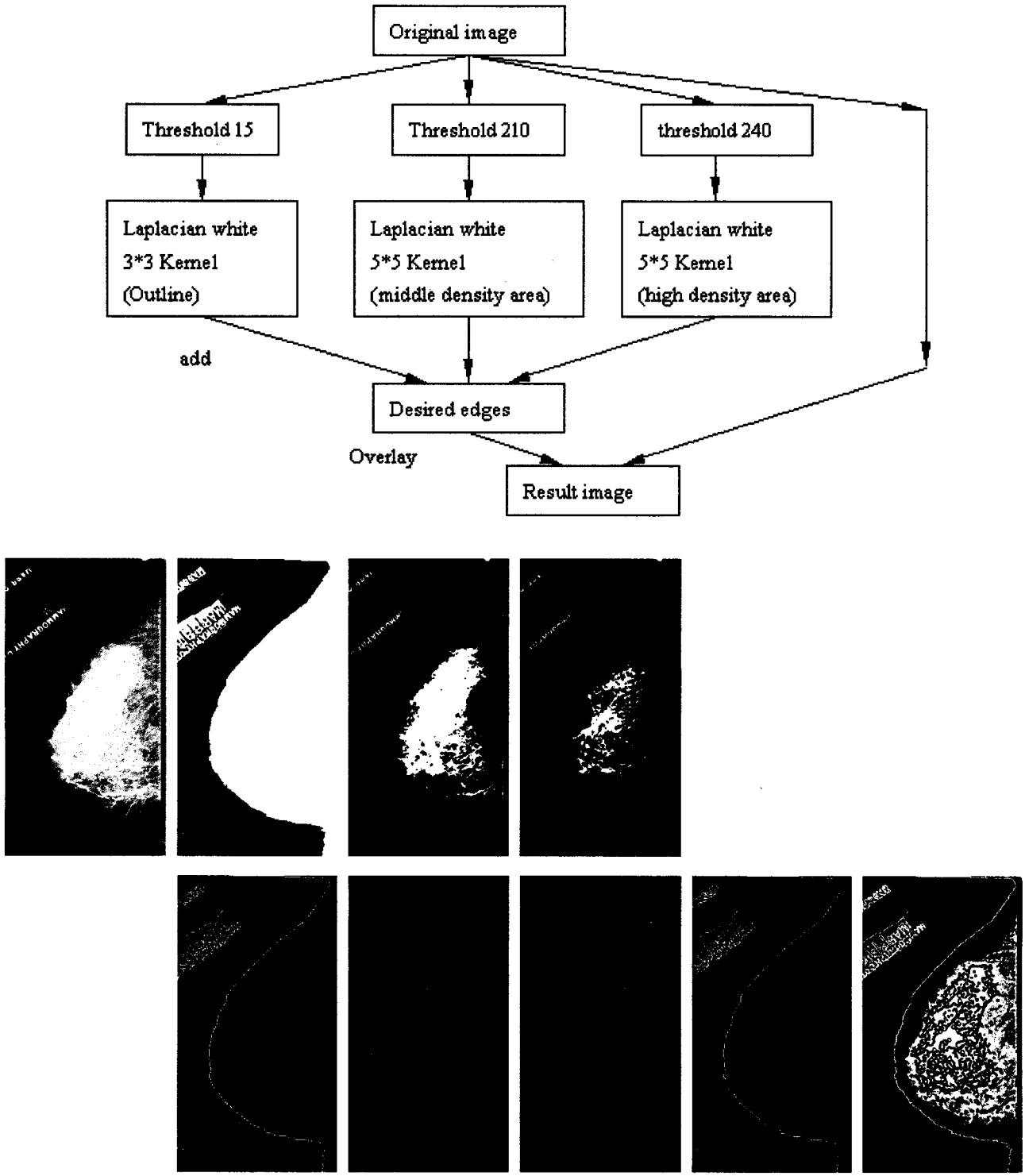
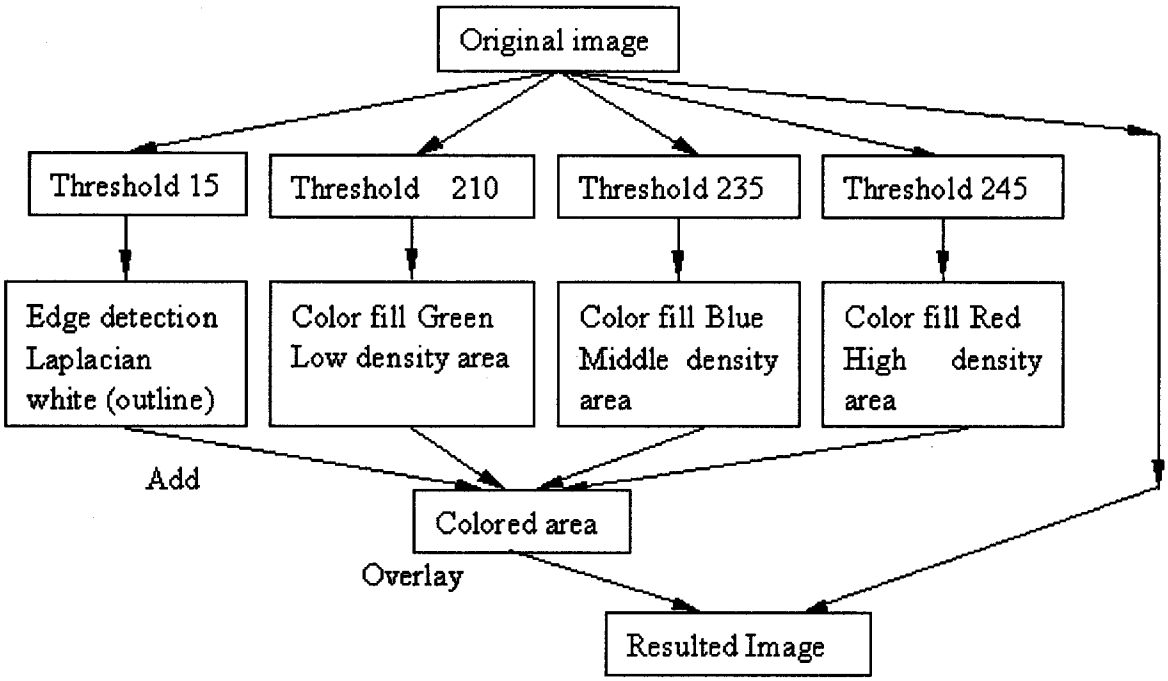


Figure 2.10: Visualization Pipelines for separating different lightness areas.

We can enhance the rendered areas by filling the segmented areas by different colors. Figure 2.11 illustrates the new visualization pipelines.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



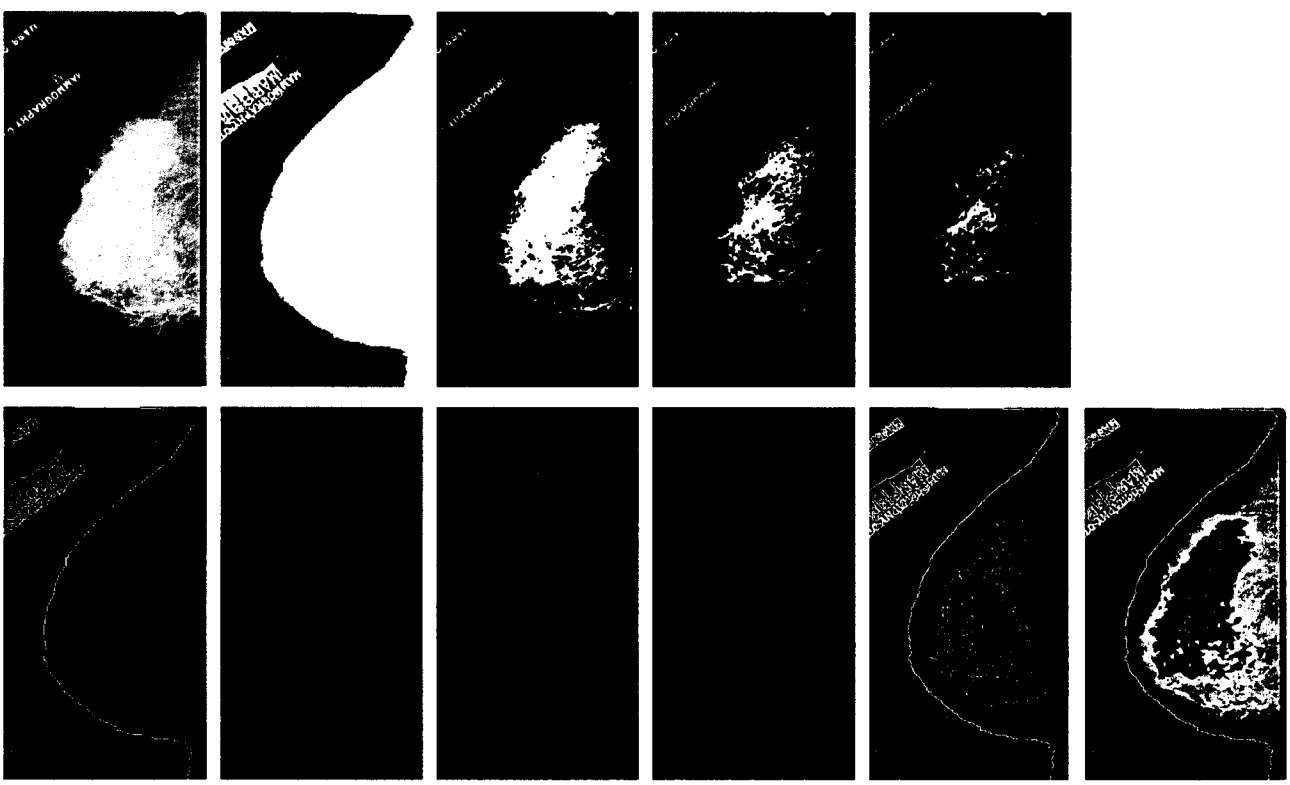


Figure 2.11: Visualization Pipeline with Area Filling Rendering Effects.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Although the result of pipelining was encouraging, a key step in this method needs to be improved. The first step of the proposed Visualization Pipeline includes several threshold operations. The best threshold values for each mammogram are different. Currently these values are manually selected by playing the thresholding scroll bar. We are now working on a dynamic threshold algorithm which will find the best values automatically.

The Visualization Pipeline operation is a good tool for Image processing experts but it is difficult to be used by the health workers. For this purpose we dedicated the next section for developing a single an effective techniques that can be easily used by the health workers. This new approach is not based on the traditional approaches centered on convolution but it is rather oriented towards sensing the fuzzy nature of the mammogram regions. We called this new approach as the Dynamic Fuzzy Classifier (DFC).

2.4 Developing an effective approach for detecting mammography abnormalities

One of the most important steps in digital mammography is an adequate segmentation of possible abnormalities. This obviously minimizes errors in further stages such as in classification. However, several factors affect the proper segmentation of mammograms. Mammograms contain low signal to noise ratio (low contrast) and a complicated structured background. In this section we are describing a generic approach for detecting patterns of architectural distortions in mammograms that is both complete and uncommitted to any type of training. Our detection algorithm dynamically updates the pixels intensities by following their neighboring transition zone. Such approach proved to be effective for detecting the edges of all types of breast abnormalities including the Stellate.

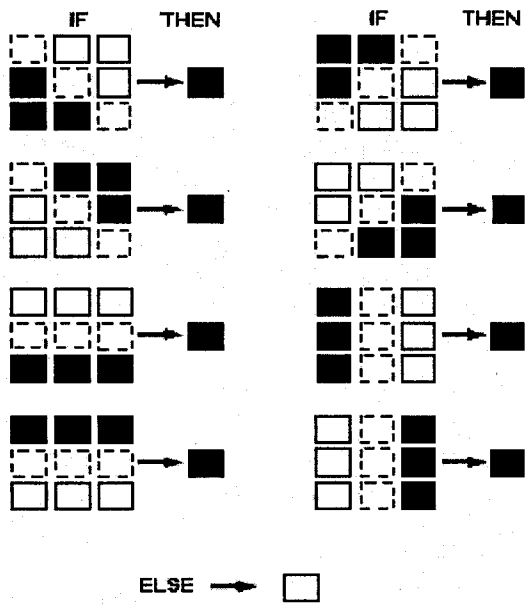
2.4.1 fuzzy edge detectors

The analysis of mammograms which usually contains non-linear noisy and imprecise data, has been a more recent research and received considerable interest over the last few years. Particularly, the use of Fuzzy techniques proved successful in several such applications as mammography since they take a more flexible approach to pattern recognition and edge detection [Tizhoosh, 1997]. Basically, there are two different possibilities for development of fuzzy edge detectors:

- By defining an appropriate Fuzzy Membership Functions [Liang, 2003]
- By defining an appropriate if-then rules in a predefined neighborhoods (e.g as in Figure 2.12)[[Looney, 2000]

However, most membership functions appeared in literature are determined heuristically without any additional rules used to modify the membership values. Indeed, the use of

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



A 3*3 mask is used to consider the effect of 8 neighbouring pixels. In the first 8 situation the central pixel belong to "0" (dark) region. Otherwise it belong to "1" (dright) region.

Figure 2.12: Rule Based Fuzzy Edge Detection.

rules can smooth while sharpening edges, but require a rather large rule set compared to the simpler fuzzy membership classifier methods [Looney, 2000]. For this purpose Neural Networks have been used to train the processes for selecting the set of rules for detecting edges [Looney, 1997] and especially the radial basis functional link nets [Looney, 2002] are found to be powerful in this direction. Training such networks is not a straightforward processes and many complications are associated with this process [van der et.al., 2003]. Moreover, these techniques proved to have high success rates in detecting some types of cancer abnormalities with systematic shape structure and in particular with Calcification Circumscribed types. However, stellate cancer lesions express vast architectural distortions and presenting with an appearance of fuzzy radiating lines. Attempts to automatically detect these abnormalities have generally concentrated on collecting some statistical features of known importance, such as textures which can be discriminated with low variances, radiating linear structure concurrency, spread of focus and radial distance. Hence, the authors believe that by developing a dynamically fuzzy membership classifier we can arrive at a simple pseudo adaptive edge detection algorithm which does not require training.

2.4.2 Dynamic Fuzzy Classifier Method:

The DFC is intended to be a part of a soft tissue abnormality detection scheme. Design of the algorithm is based on two main properties of mammographic lesions and patterns. Firstly, because of the unclear boundaries of the parenchyma and malignant masses in a mammogram, employing the principles of fuzzy sets in assigning the image pixels to different regions is appropriate. Secondly, since abnormal tissue lesions and masses are usually larger than a certain size, in determining which segmented region a pixel belongs to, the effects of its neighbouring pixels as well as its own intensity value must be considered.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

The DFC method starts by moving a polygon mask on every pixel of the given image. Each pixel will be placed at the centre of the polygon (Figure 2.13).

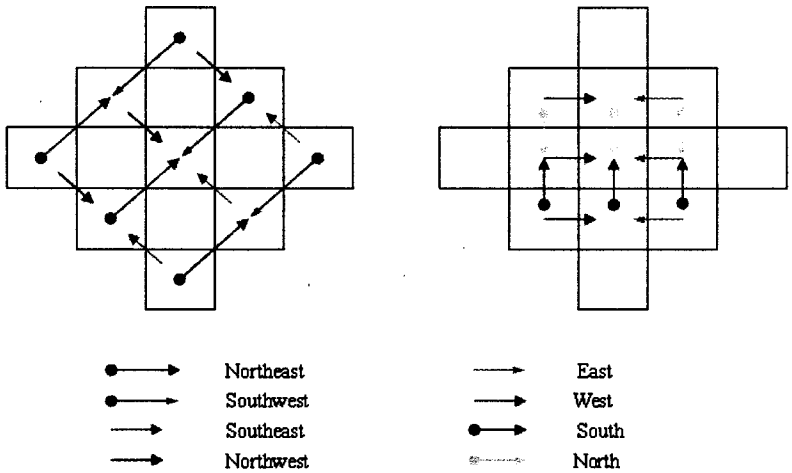


Figure 2.13: Pixel Direction Polygon Mask.

Based on the values of the brightness of the 13 pixels of the polygon, eight brightness direction features are extracted. These features are the magnitudes of the differences between the thirteen neighbouring pixels. Using the values within the polygon, we can calculate the direction features by taking the different 2x3 orientations within the neighbouring pixels within the polygon. For example, to calculate East direction feature value, we need find the value of P2-P1 + P5-P4 + P8-P7 (See Figure 2.14). The eight features direction values can be calculated in this way.

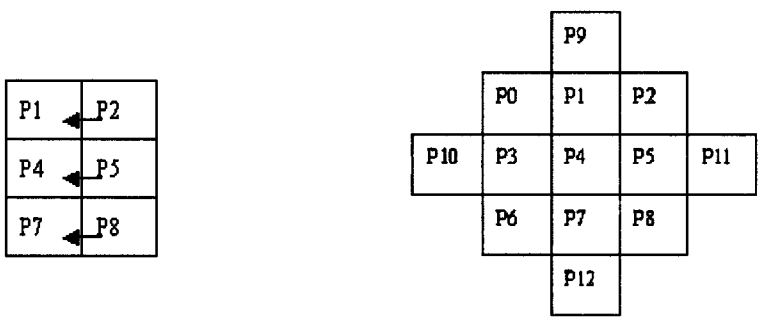


Figure 2.14: Polygon Reference Map and the East Direction Feature computation.

And for the northeast direction feature, we need to find the value of P9-P0 + P2-P4 + P11-P8 (see Figure 2.15).

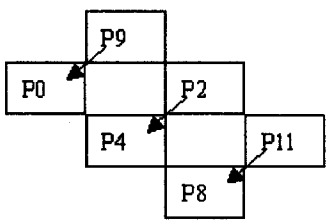


Figure 2.15: Northeast Direction Feature Computation.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

These eight direction features are the input to a fuzzy membership classifier that connect to two fuzzy set membership functions that represent set of pixels which belong to "0" (dark) region, and the set of pixels which belong to the "1" (bright) region. The membership value determines how close a pixel is to becoming a member of either set as well as the brightness slop direction. From the eight direction features we choose the highest value which will indicate the slop direction.

At each pixel, the fuzziness measure of each pixel is dynamically updated to reduce the error function value. Inspired by the Gradient method and the back-propagation algorithm for neural network training, three update rules are designed to both reduce the error in each pixel iteration and to consider the effects of brightness for all the neighbouring pixels:

Rule 1: If the direction value bigger than a brightness constant (e.g. 250), **Then** set this pixel brightness (P4) to white, **Otherwise** apply rule 2.
Rule 2: If the direction value greater than a mammogram threshold value, **Then** apply rule 3; **Otherwise** set this pixel brightness (P4) to black.
Rule 3: To apply this rule, compute the followings:
1. Choose n; odd number of pixel along the line of the slope direction of this pixel (P4). This pixel should be in the centre. The value of n should not be greater than the min (Image Width, Image Height).
2. Put the pixel values of this line to an array A[]. We call this array a transition zone.
3. Calculate the average value of array A[] elements(i.e A[0]+A[1]+....+A[n])/n);
4. Calculate the brightness transition zone width. Then calculate the array accumulation value inside the transition zone (i.e. A[1]-A[0]+A[2]-A[0]+....A[n]-A[0]).
This rule states that **If** the Average value equal the pixel value **and** the Accumulation value is greater than n + (contrast constant), **Then** set this pixel value (P4) to white; **Otherwise** set this pixel value (P4) to black.

In short, we can summarize our DFC as follows:

1. Find the slope direction
2. If the slope value on this point is very high, set this pixel to white
3. Else if the slope value is greater than a threshold value, (a) calculate the transition zone width, is this point in middle of the transition zone? (b) Calculate the accumulative rise/descend, Is the accumulative value significant?
   If both (a) and (b) yes, and the transition zone is not too wide, set this pixel white. Else set this pixel black.
4. Else set this pixel black.

The proposed DFC Method introduce the concept of fuzzy contrast that depends on how far the membership functions are stretched by an operator with respect to the middle point from data points within the transition zone being considered. The pixel orientation and

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

slope of the transition zone provide the most important information which are used for determining edge membership. Indeed the ideal case of an edge pixel is when this pixel is right at the middle of the slop of the transition zone (see Figure 2.16a). However, we always can not find a pixel is exactly in the middle. (see Figure 2.16b) In order to get a better connectivity of detected edges, a thresholding b is used: $0.8 < b < 1.25$, where b=midvalue/P4 brightness value, midvalue=(A[0]+A[n-1])/2. Rule 3 is responsible for identifying this case. Also in many cases the brightness changes sharply and the middle pixel cannot be directly specified. We call such cases as absolute steps. Rule 1 is designed to find edge pixel for absolute steps (see Figure 2.16c). An absolute pixel case is an edge if brightness increased sharply along pixel direction.

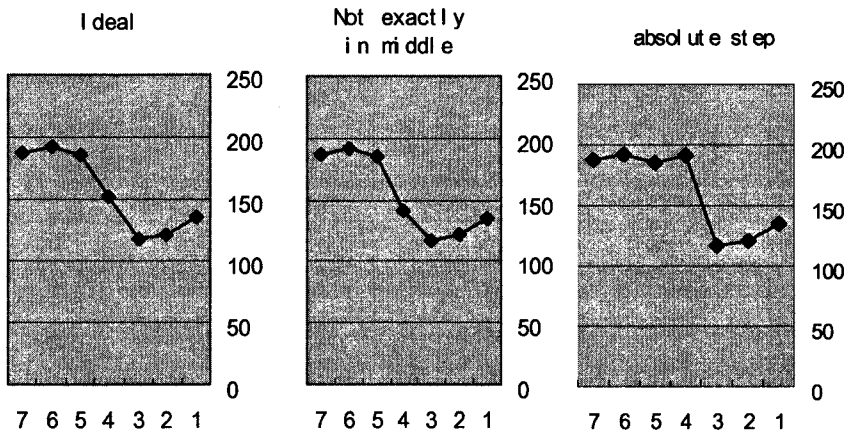
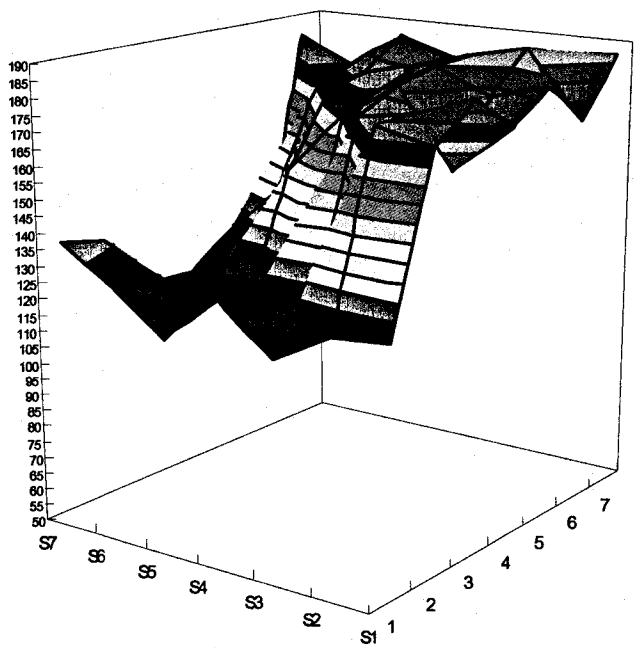


Figure 2.16: Ideal and Absolute Edge memberships



125	175	185	174	183	170	187
123	179	179	159	178	192	186
113	128	176	182	185	186	180
127	127	122	171	176	181	181
112	127	117	152	173	177	186
125	121	111	122	139	169	175
135	132	114	113	123	119	183

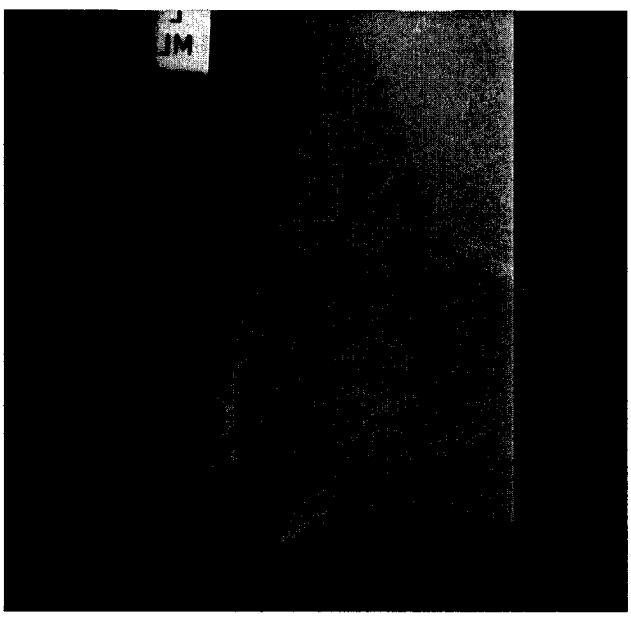
Figure 2.17: 3D Projection of Pixels Brightness.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

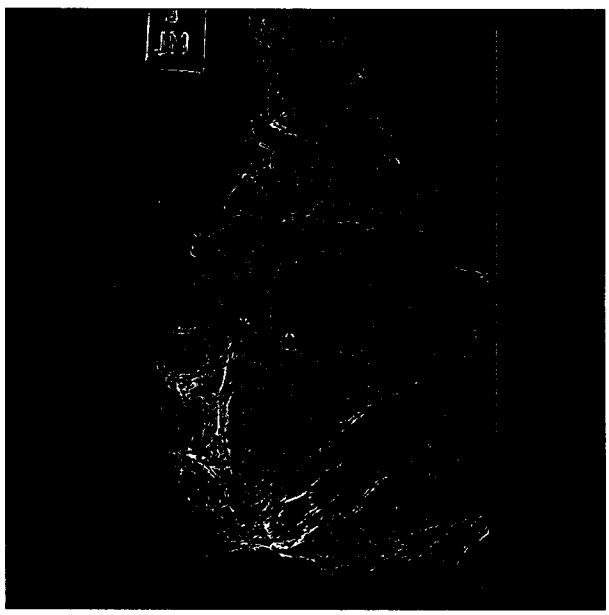
The DFC method tries to intensify the contrast of those pixels which are almost or near the actual edge. The fuzziness nature of the pixels brightness can be depicted from a 3D projection to the pixels brightness of an image segment (see Figure 2.17).

2.4.3 Experimental Results:

The data collection that was used in our experiments was taken from the Mammographic Image Analysis Society [MIAS]. This same collection has been used in other studies of automatic mammography classification. Its corpus consists of 322 images, which belong to three big categories: normal, benign and malign. There are 208 normal images, 63 benign and 51 malign, which are considered abnormal. In addition, the abnormal cases are further divided in six categories: microcalcification, circumscribed masses, spiculated masses,ill-defined masses, architectural distortion and asymmetry. All the images also include the locations of any abnormalities that may be present. The existing data in the collection consists of the location of the abnormality (like the centre of a circle surrounding the tumour), its radius, breast position (left or right), type of breast tissues (fatty, fatty glandular and dense) and tumour type if exists (benign or malign). All the mammograms are medio-lateral oblique view. Figure 2.18 shows experiments conducted on abnormal breast cases from that database with threshold value fixed to be 12. The DFC results are produced without using any preprocessing to increase the contrast or to reduce the image noise. Figure 2.18 shows two other notable edge detection methods applied on the same original image.

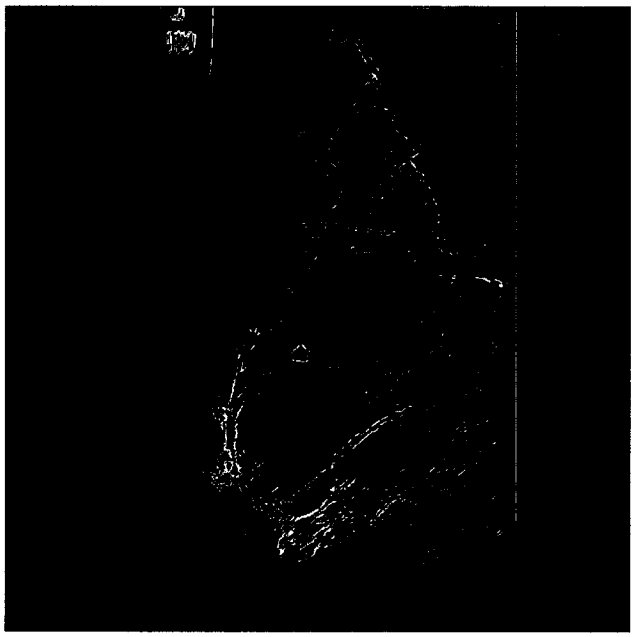


Original Image of Case #1
Circumscribed Cancer

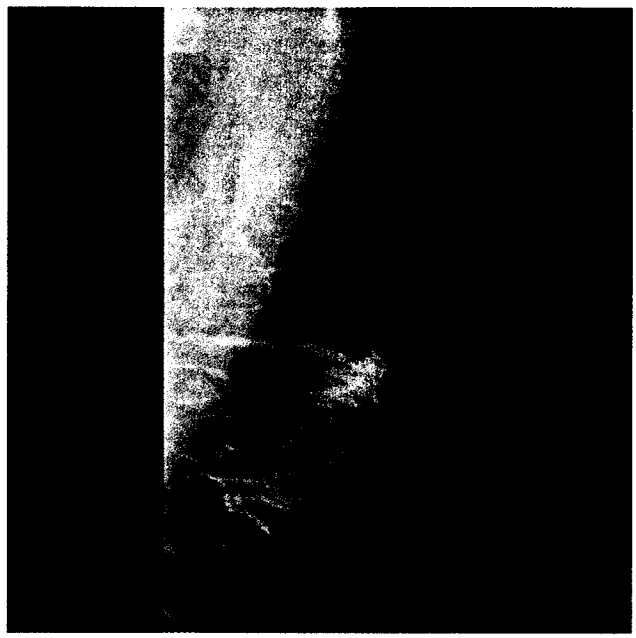


DFC Threshold=12

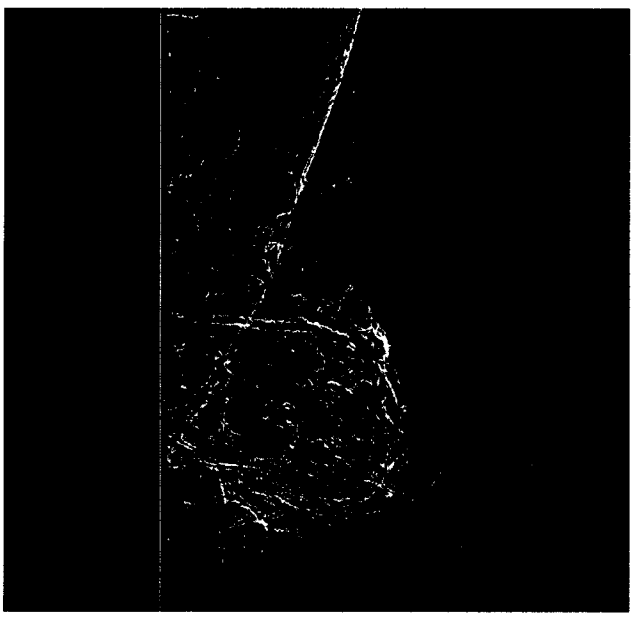
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



DFC with Threshold=12, with coloring



Original Image Case # 2: Stellate Cancer



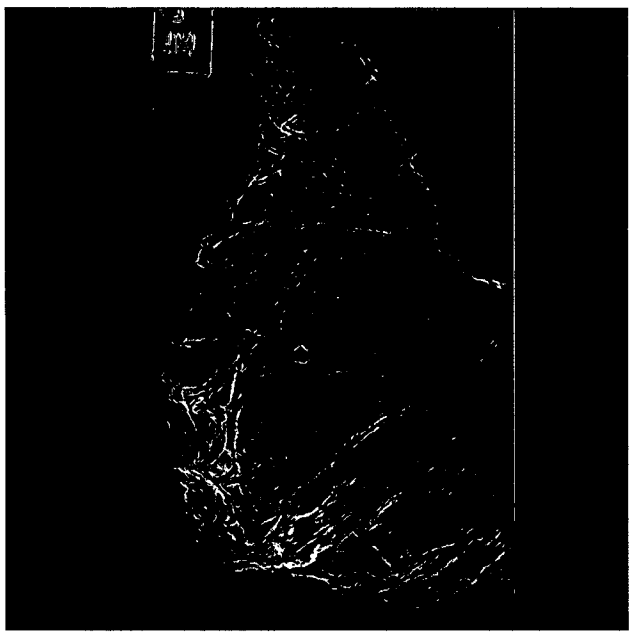
DFC with Threshold=12

DFC with Threshold=12, n=25 With Coloring

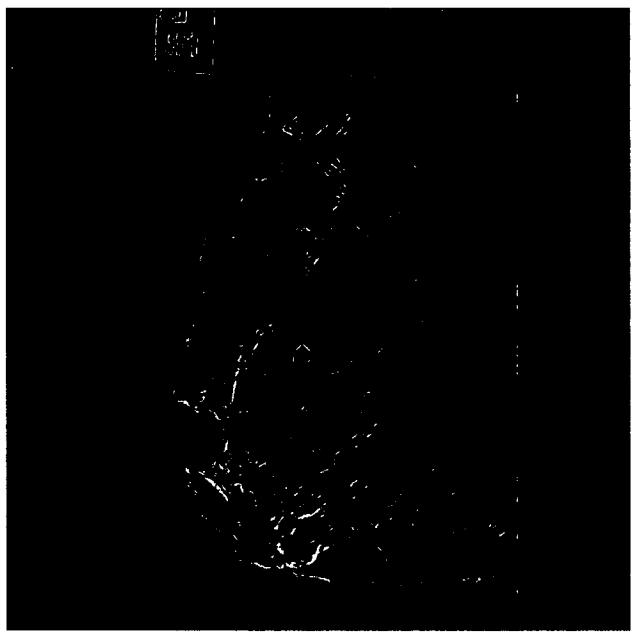
Figure 2.18: DFC Method applied on Two Mammogram.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

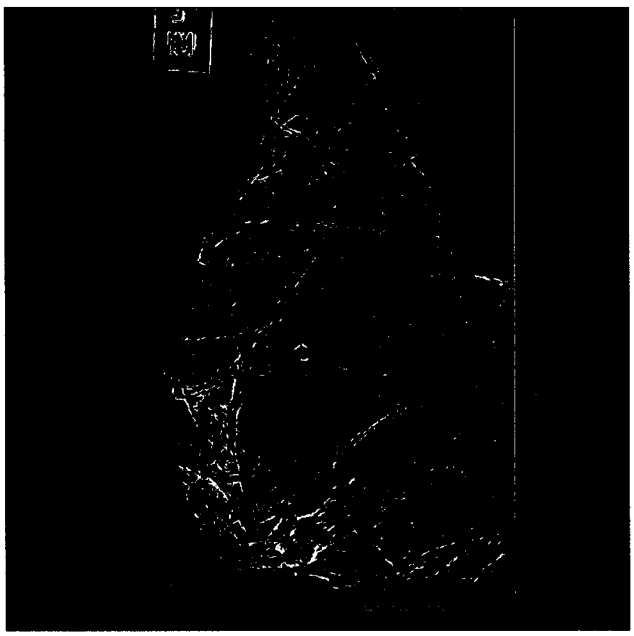
We can further more reduce noise as well as non-significant details by applying a smooth filter before DFC operation. See Figure 2.19.



Applying Median blur before DFC



Applying Gaussian blur before DFC



Applying a morphology erosion before DFC

Figure 2.19: Effect of DFC Method with smooth filters.

It is a well-known medical fact that dense breast tissues on mammograms indicate higher

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

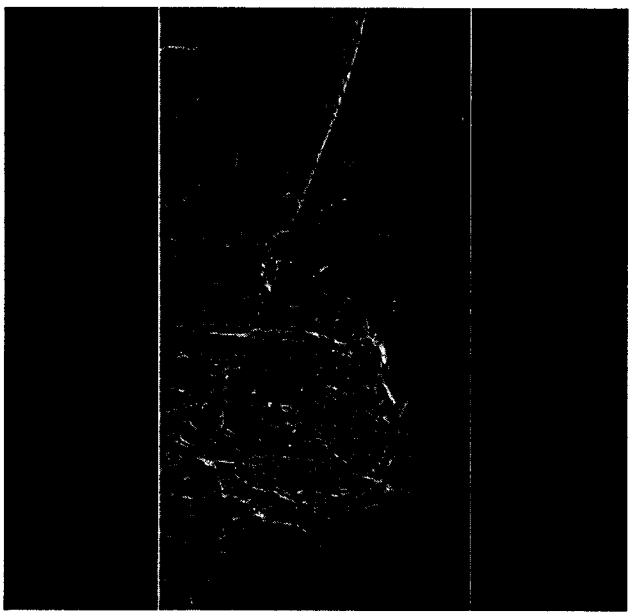
cancer risk [Halls, 2003]. A dense region, in any mammogram, always has high brightness values. For this reason, we visualized those low brightness edges to some different colors than those edges of high brightness. In this direction, we used *blue color* to identify normal regions edges (i.e. no possibility of having cancerous tissues or 0% Density Type in the radiologist terminology). *Green* has been used to identify those edges with more dense regions indicating higher possibility of having cancerous tissues (50%-74% Density Type). Finally, *White* is used to identify very high possibility of having cancerous tissues (75%-100% Density Type). We can consider this colorization process is an additional rule which is based directly on the detected edge pixel brightness. Indeed, we tested DFC on all the normal cases of the database, none of then been revealed specious structures with white or green colors. We are not claiming that the colorization scheme can be used to classify mammograms, but we can use it as one associative rule for mining abnormal mammograms. This issue is our current research program where we are trying to construct a data mining technique based on association rules extracted from our DFC method for categorizing mammograms. We are also intending for the purpose of mammograms categorization to use other measures besides our DFC association rules like the brightness mean, variance, skewness, and kurtosis for the DFC segmented image. These measures have been reported to have some success in identifying abnormal mammograms [Antonie, 2001]. Moreover, the authors experimented with all the edge detection techniques used in Table 2.1 and proved no single method can be as effective as our current DFC method [Mohammed et.al., 2003].

Mammography Method	**Reference**
Grey Level Thresholding_	[Davies, Dance, 1992]
Comparing Left & Right Breasts	[Giger, 1993]
Compass Filters	[Maxwell, Brubaker, 2003]
Laplacian Transform	[Hingham, et.al., 1996]
Gaussian Filters	[Costa, Cesar, 2000]
Texture & Fractal Texture Model	[Undrill, et.al., 1996] [Guillemet, et.al., 1996]
A Space Scale approach	[Netsch, 1996]
Wavelet techniques	[McLeod, et.al., 1996]
Mathematical Morphology	[Neto, et.al., 1996]
Median Filtering	[Bovik, et.al., 1987]
Box-rim Method	[BAZZANI, et.al., 2000]

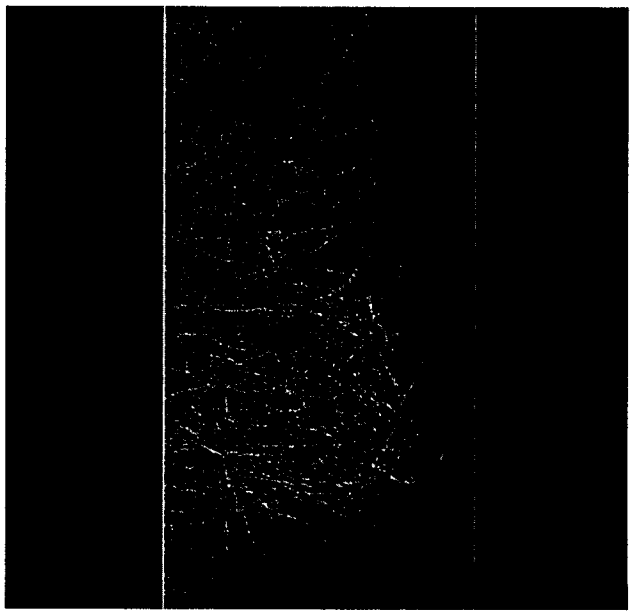
Table 2.1: Traditional Mammography Techniques.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

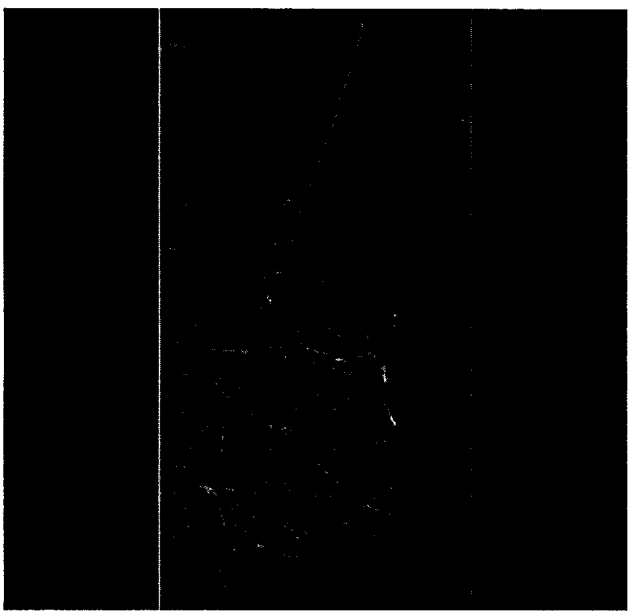
Figure 2.20 illustrates some of such comparisons for the same Stellate cancer image of this article.



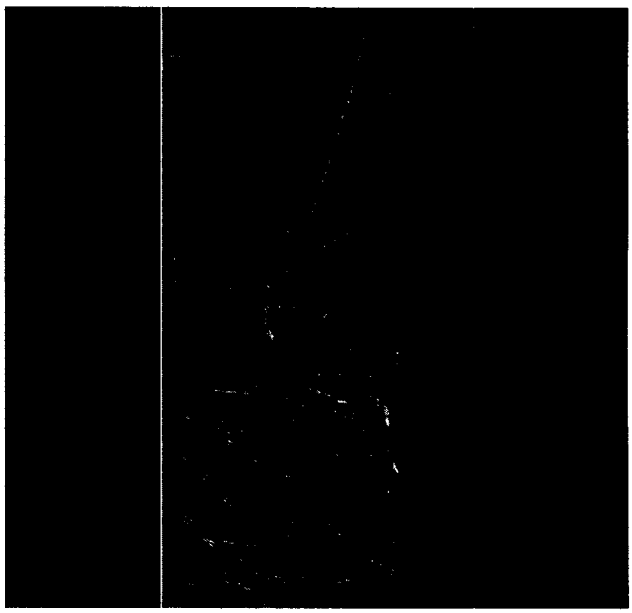
Applying Kirsch Edge Detection Technique



Laplacian Edge Detection Technique

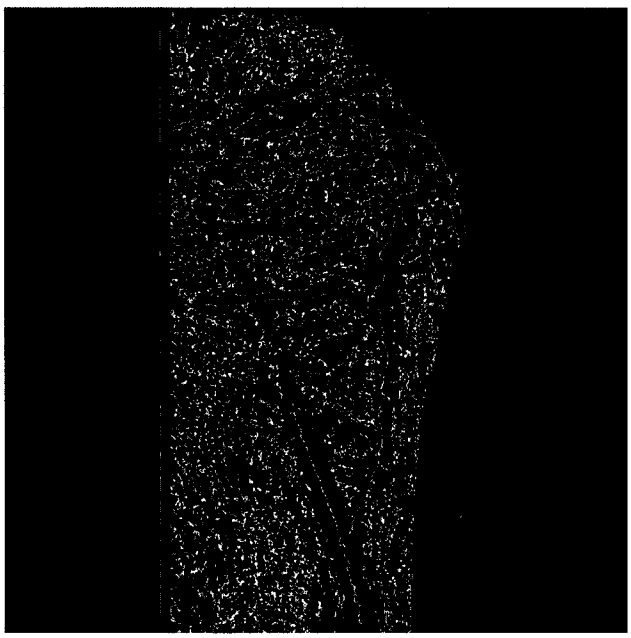


Sobel Edge Detection
With Contrast Enhancement



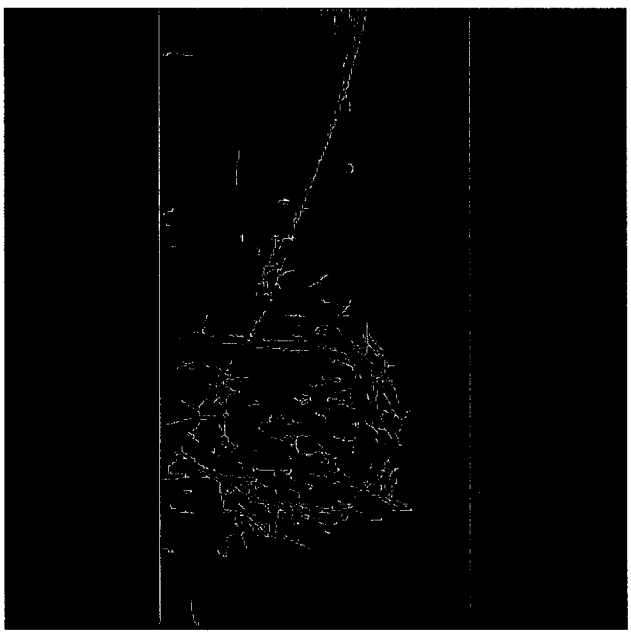
Prewitt Edge Detection
With Contrast Enhancement

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



Caffori Edge Detection wit inner window=3 and out window=31

Canny Edge Detection, Sigma =0.045



Canny Edge Detection, Sigma =0.065

Figure 2.20: Results of other Traditional Edge Detection Techniques.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

2.5 Conclusions:

In this chapter we analyzed all the conventional image processing techniques on mammograms and found no one is good enough if applied singly. A better recognition can be achieved by applying several different techniques through a pipelining sequence. Although this visualization pipeline operator is a powerful tool, it is difficult to be widely used because of its complexity. This problem can be solved by further research. On the other hand, by carefully study the nature of mammograms we presents a new membership function that transforms the intensity of a pixel into the fuzzy domain according to the direction of brightness slop in its neighboring transition zone. A new intensification operator is introduced based on a polygon for determining the corrected intensity value for any pixel. The membership fuzzification classifier dynamically evaluates every pixel's brightness by optimizing their contrasts according to the neighboring pixels. The method needs no preprocessing or training and does not change brightness nature of the segmented image compared to the original image. The DFC method has been tested on a medical mammography database and showed to be effective for detecting abnormal breast regions. In comparisons with the traditional edge detection techniques our current DFC method shows significant abnormalities details, where many other methods (e.g. Kirsch, Laplacian) revealed irrelevant edges as well as extra noise. For Sobel and Prewitt , the original images results as completely black. With contrast enhancements, Sobel and Prewitt still show extra edges and noise. With more sophisticated methods like Canny, one must have high experience to choose the various parameters (e.g. Sigma, High and Low Thresholds) and frequently adjust the threshold afterwards on the resulted image. However, using Canny method still we are seeing some noise associated with the detected edges. Moreover, with more simpler edge detection techniques like Cafforio method [Cafforio, et.al., 1997], the result is completely full of noise. Moreover, we believe that our DFC technique can be used to generate association rules for mining those abnormal mammograms. This will be left to our future research work.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Chapter 3

Developing the Mammography Consultation System Communication Infrastructure

3.1 Introduction:

Distributed computer systems are becoming ubiquitous media for information exchange. Consequently, there is great demand for, and much research on information coordination and integration mechanisms among heterogeneous, distributed and dynamic information sources. In addition, researchers are beginning to focus on mechanisms that allow end users to participate in distributed information networks without much technical support and sophisticated computing platforms. Especially in the distributed health care system involving physicians, hospitals and pharmacies who work autonomously, but regularly need to collaborate and exchange patient information. Such situation is served well by using a peer to-peer computing environment. This environment, popularized by systems such as Napster and Gnutella, views a distributed system as an open, dynamic network of *peers*. Each peer is *acquainted* with a small number of other peers with whom it can exchange information and services. Acquaintances change constantly, there is no central control/registry, and peers remain autonomous throughout their participation in a P2P network. There is also no support for wireless and ubiquitous devices such as 3G Mobile Phones, PocketPCs, LapTop PCs and PDAs which are becoming more popular in the health care system.

As more and more advanced medical equipment is used in diagnosis and management of disease, it is becoming increasingly difficult to maintain and retrieve health care information manually. In particular ubiquitous technologies can speed the process of consultations among doctors, specialists and health workers. Doctors and nurses are always on the go. Having a ubiquitous communication environment will give them the ability to communicate wherever, whenever they wish. On top of that computing technology can assist in providing essential primitive diagnostic information especially when dealing with complex spatial data such as X-Ray images. This chapter focuses on developing a secure instant messenger infrastructure for this purpose. The infrastructure presents three channel architecture where instant messages and image files can be sent separately in a secure way. Because of the ubiquitous nature of this architecture, the instant messages will be sent/received based on the XML channel, the Image files will be transmitted via the TCP/IP channel, and both previous channels will be secured via the SSL channel/protocol. With this infrastructure, doctors can discuss their diagnose opinions ubiquitously and in real time. At the same time they can exchange records, documents, and mammograms. Every doctor can communicate with more than one doctor. Thus many doctors in different place of the world can easily work on one case using this

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Mammography Consultation System through Internet.

However, we distinguished two main components in this infrastructure: the server and the client. Figure 3.1 illustrates a general view of our developed infrastructure.

3.2 XML Message Channel:

This channel is an XML messenger [Deite et.al., 2001]. It is based on client-server model and utilized the general TCP/IP protocol. Clients, or user of the system, are the people who need to communicate with other users in the system. Consider a case where user 1 needs to communicate with user 2. For communication to be established, both users need to be logged on to the server. The messenger displays all the users who are currently log on to the server. User 1 can then choose to send message to user 2. When user 1 types in a message for user 2, the message is tagged with XML and sent to the server. The XML message also contains the destination (User 2) of the message and its source (user 1). The server then reroutes the message to the respective user based on the destination information provided in the message. The design details of both the server and client sides of the XML messenger are described in the following two sections. Figure 3.2 illustrates the general GUI for our Infrastructure where the XML messenger can appear as one of its communication channels.

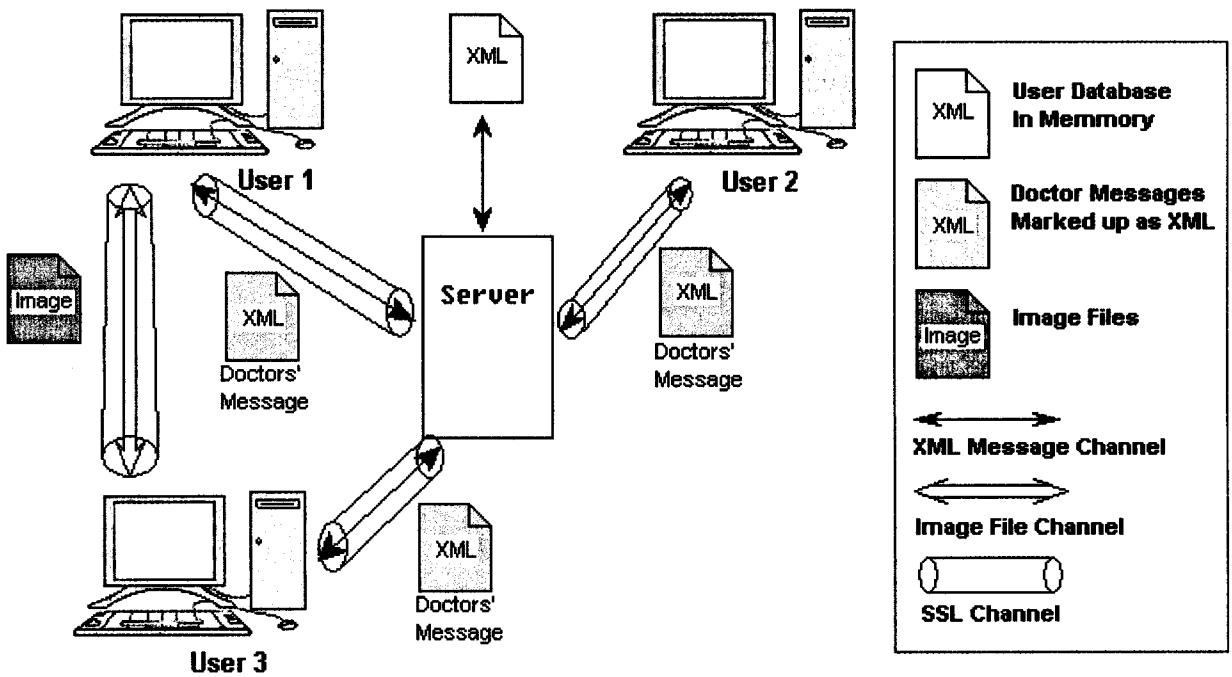


Figure 3.1: XML Messenger Architecture

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

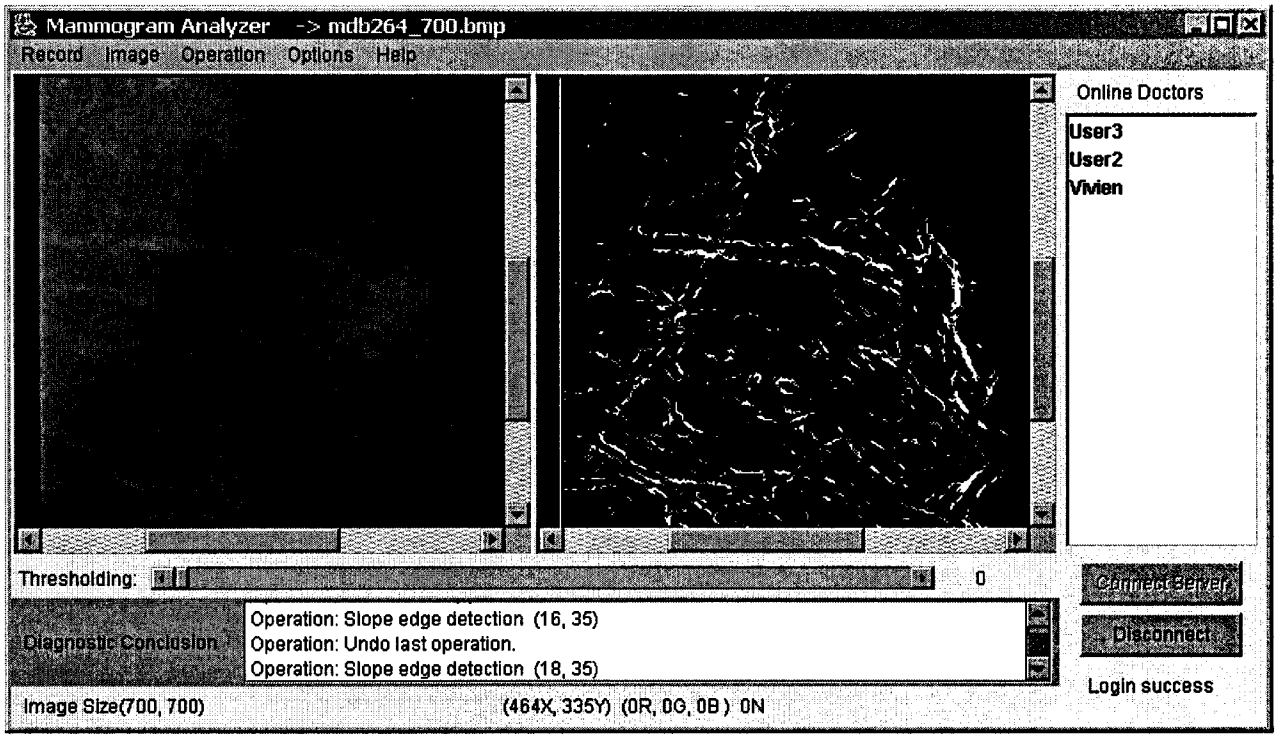


Figure 3.2: The infrastructure GUI.

3.2.1 The Server of the XML Messenger:

Using a ServerSocket, a MessengerServer object waits for clients to connect. When a client connects, the server creates a new UserThread object to manage the client's socket and streams. The MessengerServer object uses a vector to store all UserThread instances.

The MessengerServer also uses a Document object users, consisting of the names of on-line users stored in individual user elements. For example, after User1 and user2 have logged in, the server's Document users is

```
<users>
    <user>User1/user>
    <user>User2</user>
</users>
```

When a user first logs in, an XML document is sent to the MessengerServer object's corresponding UserThread object as

```
<user>username< /user>
```

The UserThread object processes all incoming messages; when it receives this message, it tests if username has already been taken by another user. If so, the UserThread object sends the client an XML document containing

```
<nameInUse />
```

If username is not in use, the UserThread object sends the client the MessengerServer object's Document users. The MessengerServer then notifies all other users of this new user's login by sending them the XML document

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

<update type = "login">
<user>username< /user>
</update>

If the user sends a message to another user, the corresponding UserThread object receives an XML document with root element message. For example, if User1 sends "hello" to User2, the following XML is received by the UserThread corresponding to user1

<message to = "User2, from = "User1">hello</message>

When the userThread object receives the XML, it relays it to the MessengerServer for appropriate routing. The MessengerServer object then sends the above XML to the user referenced in the to attribute.

The last XML document the UserThread object receives from the client is sent when the user disconnects. This XML document contains

<disconnect/>

When this XML message is received, the MessengerServer object notifies all other users that this user has logged out by sending them the following:

<update type = "logout">
<user>username< /user>
</update>

Class MessengerServer implements the server for the xmlmessenger application. Vector onlineUsers stores the individual UserThread objects, which represent the individual users. The names of all users are stored in the Document object referenced by users. Each user is stored in a separate user element, as in

<Users>
<user>usemame1 </user>
<user>usemame2< /user>
</users>

This Document is sent to every new user that logs in and is updated whenever a user logs in or out.

Moreover, the constructor creates the GUI; note that class MessengerServer extends class JFrame. It also initializes the instance variables; when initializing the Document users, it invokes the private method initUsers, which creates a new Document. We then create the root element users and append it as the child of the Document object referenced by init. Note that a Document object can have only one child -- its root element.

Method runServer is invoked by method main. It creates a new ServerSocket server, which waits for clients to connect. When server receives a connection, method accept returns a Socket object specific to the client. This Socket object is then passed UserThread's constructor. Class UserThread extends class Thread. By managing each client as a separate thread, the server can handle more than one client at a time.

When a new user successfully logs in, method adduser is invoked. We notify all users of this

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

user's login using method updateusers. Add the user to the users Document by creating a new user element and setting its contents to the specified username. Finally, we add the passed userThread object to the Vector onlineUsers; note that we do not want to add it until a successful login has occurred, since the user is not officially online until that point.

Method sendmessage is invoked when a message from one user to another is received by the sender's UserThread. Parameter message references a Document object containing the message in the form

```
<message to = "receiver" from = "sender">
    message text
</message>
```

We traverse the DOM to access attributes to and from to determine the receiver and sender of this message, respectively. Local variable index stores the index of the UserThread corresponding to the receiver in the vector onlineUsers. To initialize index, we call helper method findUserIndex. This method searches the Vector onlineUsers for the userName. When a match is found, the index is returned; if there is no match, -1 is returned. Using index, sendMessage sends the message to the receiving client using the receiver's UserThread method send. Finally, method sendMessage calls method updateGUI, updating the server's GUI to reflect the message transfer.

Method updateUsers is invoked when a user either successfully logs in or logs out. It is used to notify all other users of the login or logout. After the root element is appended as the child of Document doc attribute type is created, and its value is set to "login" or "logout," depending on the passed String parameter type. Then element user is appended as a child to the root element. Finally, a text node containing the passed String userName is added to element user. This step creates the XML document

```
<update type = "type">
    <user>userNarne< /user>
</update>
```

When a user logs out, method removeUser is invoked. We remove the specified UserThread from the Vector onlineUsers. We must also remove the user from the Document users. To do this, we retrieve all user elements with Element method getElementsByTagName. We iterate through the resulting NodeList until we find the user element corresponding to this user. Using Node method removeChild, we remove this element from the root element users.

Class UserThread extends class Thread. A UserThread class object is created for each client that connects to the server. Variable connection references the Socket for this particular client; input and output reference the input and output streams, respectively. Variable server references the MessengerServer that instantiated this UserThread object. The client's username is stored in String username. Finally, boolean keepListening is used in a

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

while loop; a UserThread object listens to communication from the client until keepListening is set to false in response to the user's logout. Figure 3.3 illustrates the XML messenger server responding messages. Figure 3.4 provides the UML Class Diagram of our XML messenger server.

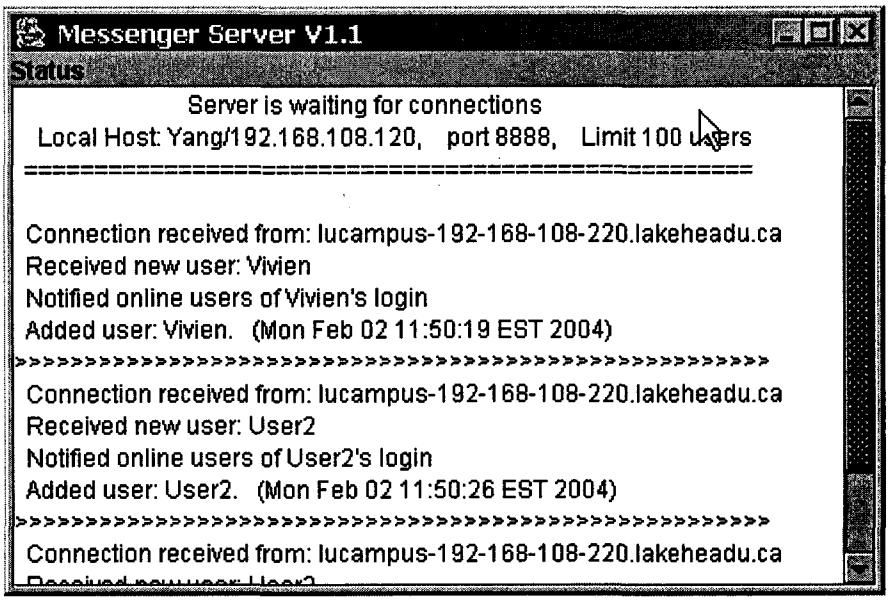


Figure 3.3: GUI of MessengerServer

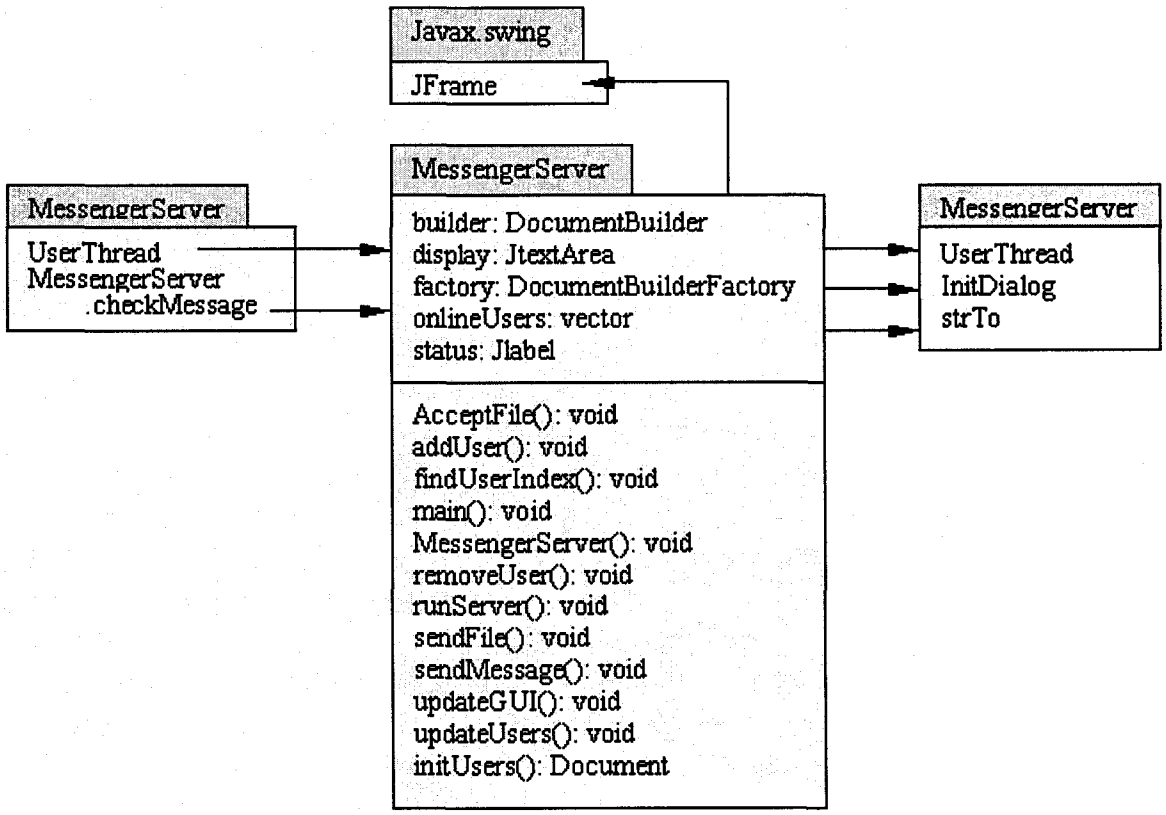


Figure 3.4: UML Class Diagram of the XML MessengerServer.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

3.2.2 The Client of the XML Messenger:

The client-side application has two main functions. First, it registers the user with the server by sending an XML document that contains the user's name and ID. It then updates its current list of logged-on users with the new information it receives from the server. During the session, that is, the period during which the user is logged on, it has to update this list whenever a new user logs in. All such information is exchanged in the form of XML. The second function of the client is to convert the text typed in by the user into XML-based messages, tagging them appropriately to identify the source and destination of each message, and to send them to the server. The client also has to parse the XML messages received from the server and display them to the user.

On the client side, a MessengerClient object connects to the server, establishing a socket. Once a connection has been made, the MessengerClient object gets the input and output streams. The user attempts to login by entering a username and clicking on Submit; the username entered is sent to the server in the following XML document

<user>username< /user>

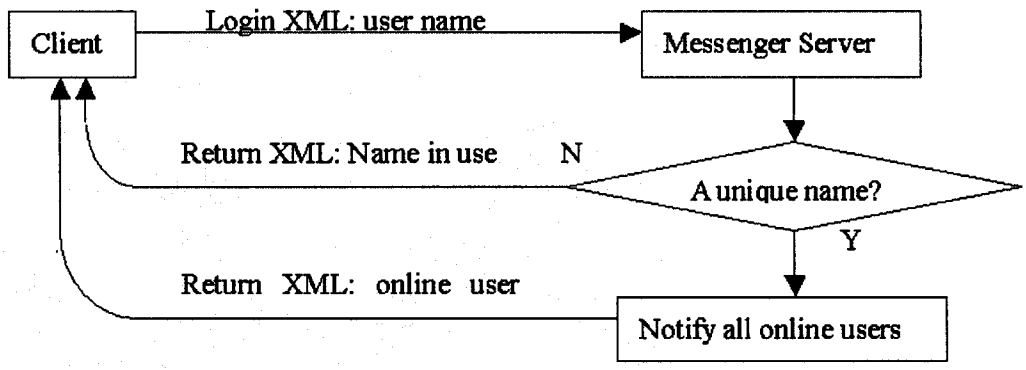
If username is already taken by another user, the server sends back the XML

<nameInUse/>

When the MessengerClient processes this message, it displays an alert dialog to the user, asking for a unique name. Once the user has entered a unique name, the server sends back an XML document containing the names of all users currently on-line. For example, if User2 and User3 are the only other users on-line, the client receives

<users> <user>User2</user> <user>User3</user> </users>

The MessengerClient object stores this XML document as a Document object for use by the ClientStatus object it creates. Client login procedure:



The ClientStatus GUI displays all users, by traversing the DOM. Because the user has successfully logged on, the Messenger Client window is hidden. The main window for the user is now the ClientStatus window (i.e., Messenger Status). When the user double clicks a name in this window, a new Conversation object is created. The Conversation object is stored in the MessengerClient's conversations Vector, allowing the MessengerClient to access it as needed.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

For instance, if User1 double clicks User2, a window pops up created by a new conversation object. When User1 types "hello" and clicks Enter, a new Document is created, containing

<message to = "User2" from = "User1">hello</message>

This message is sent to the server through the MessengerClient's output stream.
Now suppose User2 replies with "hi." The server sends User1's MessengerClient the XML

<message to = "User1" from = "User2">hi</message>

After retrieving the from attribute, the MessengerClient then accesses the Conversation with User2 and displays User2's "hi" message. Figure 3.5 illustrates the Client-Side interface of our XML messenger.

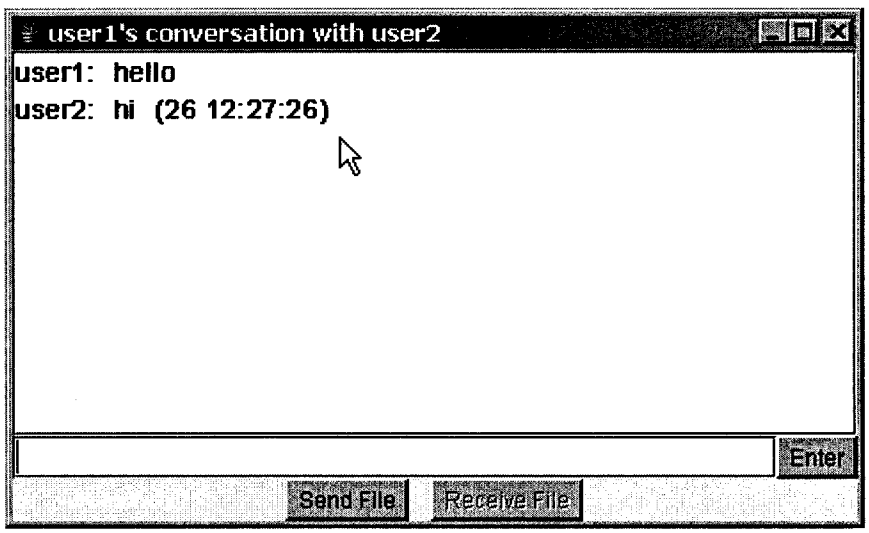


Figure 3.5: The interface of the Client of our XML messenger.

If User2 then logs out, User1's MessengerClient receives XML from the server

<update type = "logout"> <user>User2</user> </update>

User1's ClientStatus updates its onlineUsers vector and GUI to reflect User2's logout, then checks for an open Conversation with User2; if so, it informs User1 that User2 has logged out and disables the Conversation's GUI components.

If User4 logs in, a similar process occurs. First, User1's MessengerClient receives the XML update message

<update type = "login"> <user>User4</user> </update>

User1's ClientStatus then updates its onlineUsers vector and GUI to indicate that User4 is now on-line.

User1 can disconnect by clicking the Disconnect button in the ClientStatus window. This action creates and sends the XML

<disconnect/>

to server. The server terminates the connection to this client, and the client's application closes. Figure 3.6 illustrate the UML Class Diagram of the Client of the XML messenger.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Class MessengerClient establishes and maintains the client's connection to the server. As with class UserThread, boolean keepListening is used in a while loop; this allows the client to listen continually for communication from the server until the user disconnects. Variable clientStatus references the ClientStatus object that is created when a successful login occurs. We store the server's response to a successful login in the Document object users. Finally, every class Conversation object that is affiliated with this user is stored in Vector conversations.

Method runMessengerClient is called by method main. It attempts to establish a connection with the server. Once a successful connection has been made, we enable the Submit button and set boolean keepListening to true. As with the loop in the userThread class, we create a buffer to hold the incoming XML. We then instantiate a new InputSource object from this buffer, using a byteArrayInputStream. By invoking XmlDocument method createXmlDocument, we create a Document object from this InputSource. If this object is not null, it is passed to method messageReceived for processing. When the user disconnects, the while loop is exited, and the client's application terminates.

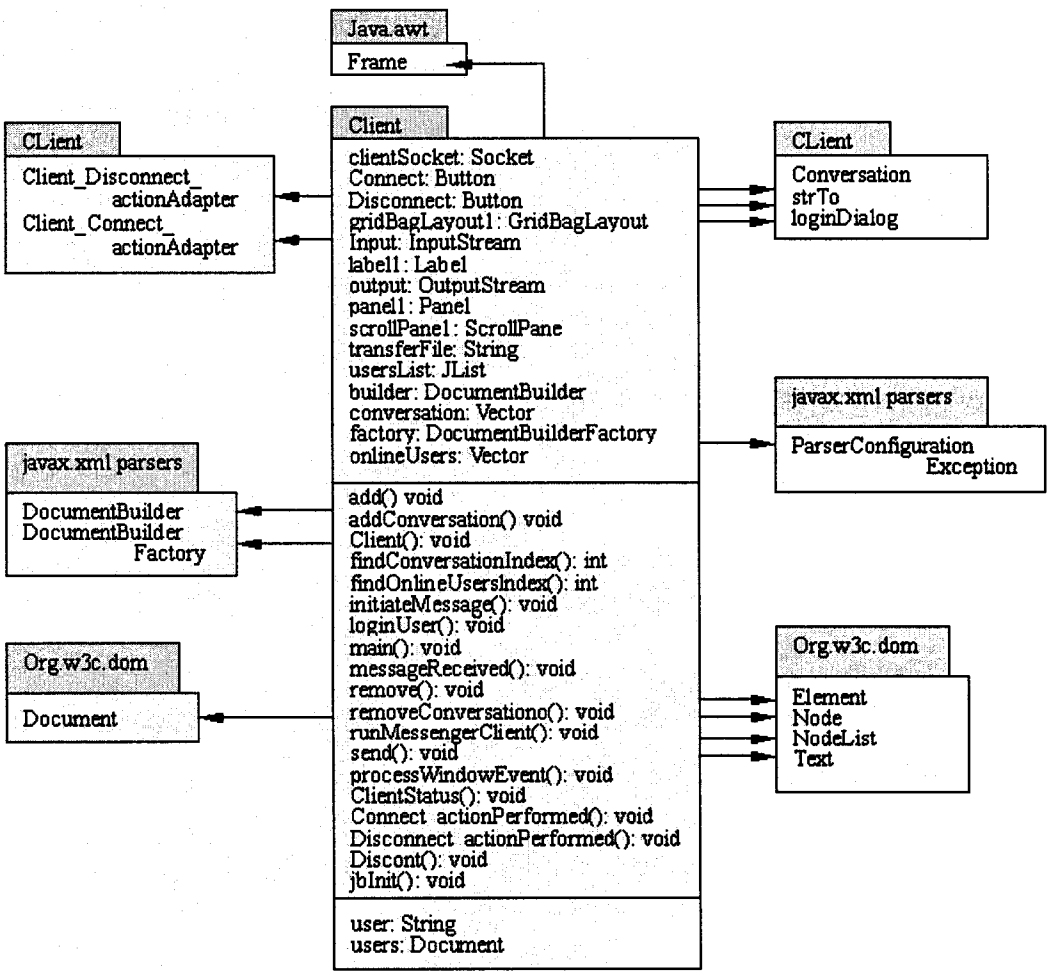


Figure 3.6: The UML Class Diagram of the XML MessengerClient.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

When the user clicks the Submit button, method loginUser is invoked. This method creates a new Document object. This step creates the XML

<user>usemame< /user>

Using method send, we send the XML to the server.

When an XML message is received, method MessengerClient passes the Document to messageReceived. Method messageReceived processes the XML from the server. First, we retrieve the root element. Then we test if it is nameInUse; if it is, then the server is responding to an attempted login by indicating that the submitted name is already in use by another user. We inform the user by displaying a dialog box asking the user to enter a unique name.

If the root is users, then the server is responding to a successful login by sending XML containing the name of all the users. We initialize reference users with the Document object for later use. Then a new ClientStatus object is created. Finally, we initialize the conversations Vector to a new Vector and hide the window for the MessengerClient class. Note that creating a new ClientStatus object displays a different window; the current login window is no longer relevant.

The server could also send XML with root update, indicating that another user has either logged in or logged out. Recall that this XML takes the form

<update type = "login or logout"> <user>username< /user> </update>

We retrieve the contents of attribute type and element user, then we test if the type attribute is login. If so, we invoke ClientStatus method add. Otherwise, the type attribute must be "logout," and we invoke ClientStatus method remove. We also check if a Conversation with the specified user exists; if so, we inform the user that the other user has logged out and disable various GUI components of the Conversation object.

Finally, the root element could be message, indicating that the user is receiving an instant message from another user. We retrieve the sender's username and text message. Then we initialize local variable index using helper method findConversationIndex. We iterate through the conversations Vector, testing if the Conversation instance variable target equals userName. If no Conversation matching userName is found, f indConversationIndex returns - 1. If index is not -1 (i.e., a Conversation with the sender already exists), we access the Conversation with the sender and display the message text. If index is -1, we create a new Conversation object with the sender and display the message text.

Methods addConversation and removeConversation add and remove the specified Conversation object from vector conversations, respectively.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Method send accepts a Document object as its parameter. We send the XML to the server via the output stream by using XML Document method write

Class ClientStatus creates the status window for the user after a successful login has occurred. Variable client references the MessengerClient object that created this ClientStatus object. We store the user's username in String name. Vector onlineUsers is used to create and update the usersList.

The constructor creates the GUI for the ClientStatus window. When initializing Vector onlineUsers, we access the client's users Document. Using Element method getElementsByTagName, we retrieve all the user elements. The onlineUsers Vector is used to initialize JList usersList. A new MouseAdapter object will be created to respond when the user double clicks a name in the usersList component. If the user double clicked a username, we call method initiateMessage. We also create an event handler for JButton disconnect; when the user clicks the Disconnect button, method disconnectUser is invoked.

Method initiateMessage first determines the name the user selected. We then test to see if a Conversation with the targeted user already exists by using ClientMessenger method findConversationIndex. If no Conversation exists, we create a new Conversation object.

Method add is invoked in response to the server informing the client that a new user is logging in. We add the specified user to the onlineUsers Vector and update the JList usersList so that the user knows that a new user is on-line.

When the server notifies the client that a user has logged out, method remove is invoked. We first remove the specified user from the onlineUsers Vector. To find the index of the element that we want to remove, method findOnlineUsersIndex is invoked. Method findonlineUsersIndex iterates through the onlineUsers Vector, returning the index corresponding to parameter onlineUserName; it returns -1 otherwise. Once the corresponding element has been removed, we update the usersList.

Method disconnectUser is invoked in response to the user clicking the Disconnect button. To inform the server that this user is disconnecting, we create a new Document object. We then create and append element disconnect. Using the MessengerClient method send, we send the XML to the server. Finally, we invoke MessengerClient method stopListening, which results in the termination of the client's application.

Every Conversation object manages an instant-message conversation between this user and another user. The clientStatus and client variables reference the ClientStatus object that created this Conversation object and the ClientMessenger object associated with it, respectively. String target contains the name of the user with whom this user is conversing.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

The constructor creates the GUI and initializes the instance variables. When the window is closed, this Conversation object should be removed from the client's conversations vector. We add this Conversation object to the client's conversations vector.

When the user hits the Enter key or clicks the Enter button, method submitMessage is invoked. First, we retrieve the text contained in the JTextField message. Then tests if the user actually entered text. If so, we create XML to send to the server; recall that it takes the form

<message to = "receiver" from = "sender"> message text </message>

We create a new Document object; then we create the root element message.Set the attributes to and from to target and the clientStatus's instance variable user, respectively. We create and append a text node containing the message text. Using the MessengerClient method send, we send the XML to the server. Finally, we update the Conversation GUI to display the entered message and clear the message JTextField.

3.3 Image Transfer Channel:

This channel is based on Java Socket programming. However, there are two Java communication protocols that utilizes socket programming: datagram communication and stream communication. Our Image transfer channel is built upon a stream socket programming. The stream socket is protocol that is based on TCP (transfer control protocol). Unlike UDP, TCP is a connection-oriented protocol. In order to do communication over the TCP protocol, a connection must first be established between the pair of sockets. While one of the sockets listens for a connection request (server), the other asks for a connection (client). Once two sockets have been connected, they can be used to transmit data in both (or either one of the) directions. Creating a socket like Socket MyClient can be done simply using:

MyClient = new Socket("Machine name", PortNumber);

Where Machine name is the machine you are trying to open a connection to, and PortNumber is the port (a number) on which the server you are trying to connect to is running. When selecting a port number, you should note that port numbers between 0 and 1,023 are reserved for privileged users (that is, super user or root). These port numbers are reserved for standard services, such as email, FTP, and HTTP. When selecting a port number for your server, select one that is greater than 1,023!

The programming techniques for this type of messenger are well-known and we refer the reader to [Mahmoud 1996]. In case of user1 wants to send an Image File to user2, user1 must use the general infrastructure GUI and press "Connect" (see Figure 3.2) and pressing "Send File"(Figure 3.7a) to the user name of User2. Before sending the actual image file, the user need to use the XML messenger to notify the other user:

<TransferRequir to = "receiver" from = "sender">

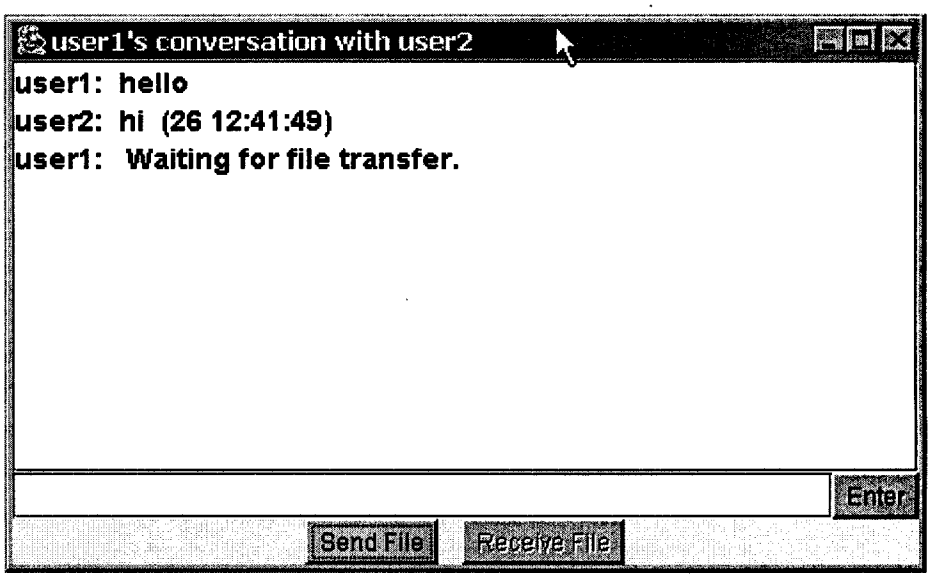
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Waiting for file transfer: (filename) </TransferRequir>

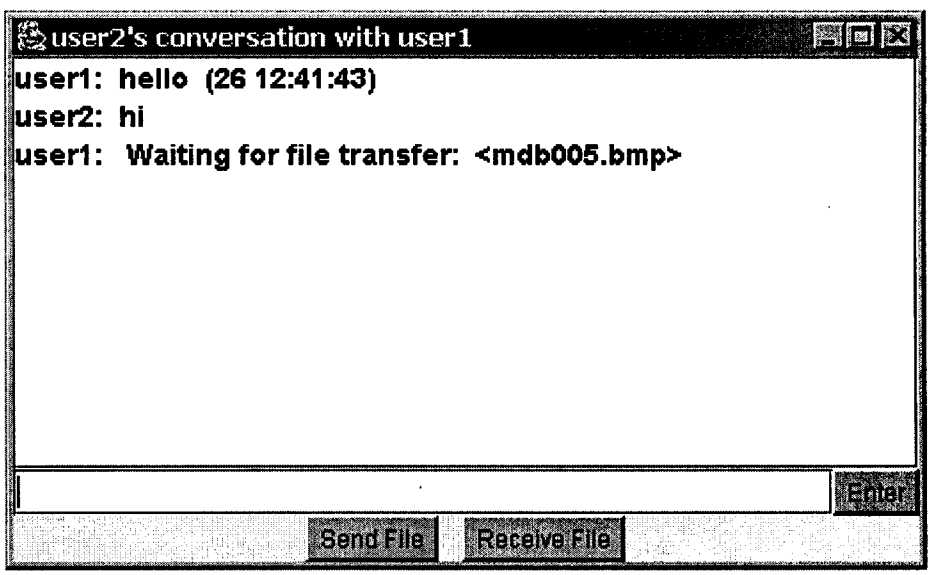
If user2 accept the file transfer, an accept message will be created and sent back to user1:

<Accept to = "receiver" from = "sender"> (IP address of user2) </Accept>

At the same time user2 create a SeverSocket and waits for incoming connection. User1 can get the IP address of user2 from the above message. Then user1 create a Socket and connect to user2 by the IP got from message. After all above success, file transfer will start. Each side will be acknowledged when file transfer finished (Figure 3.7 d, e). When server redirects it to user2, the button "receive file" will be enabled (see Figure 3.7b). User2 can choose to receive file or ignore it. Figure 7 illustrates some snap shots of conversations betweens User 1 and User2.

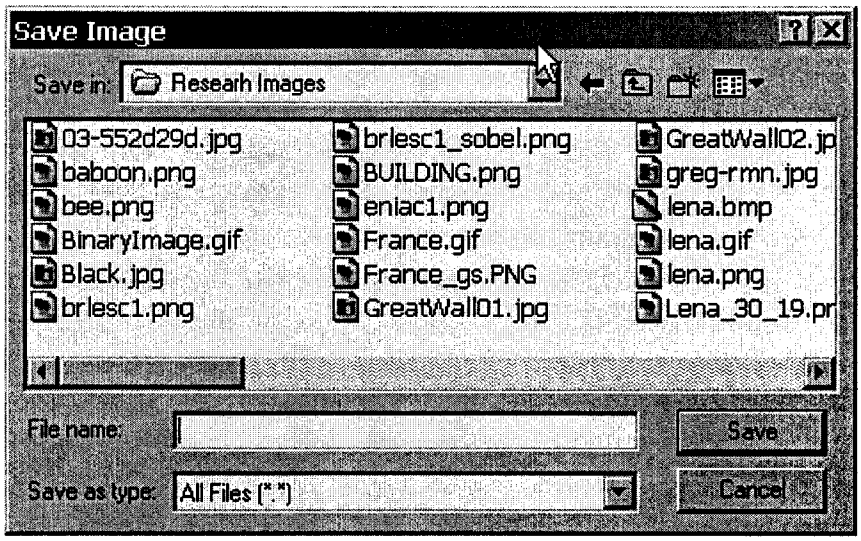


(a) User1 waiting for image transfer



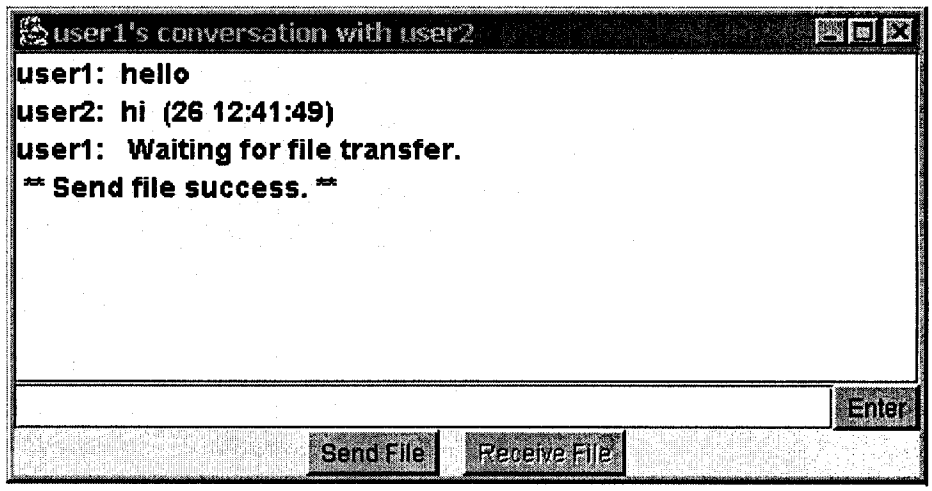
(b) User2 can choose to receive image now

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



(c) User2 need to choose a directory to save image file.

(d)



(e)

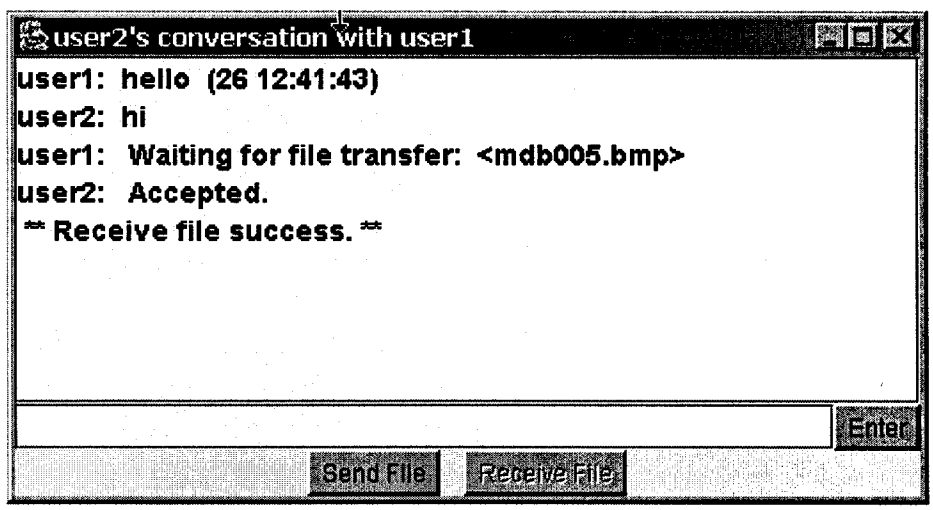


Figure 3.7: GUIs of file transfer

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

3.4. The SSL Channel

This channel will be used to secure the communications in both channels (XML Messenger and the Image file transfer channel). The SSL is a standard protocol used over the Internet. The details of utilizing this protocol is given herewith in the next section.

The SSL protocol, which was developed by Netscape in 1994, allows clients (Web browsers, typically) and HTTP servers to communicate over a secure connection. It offers encryption, source authentication, and data integrity as means to protect information exchanged over insecure, public networks. There are several versions of SSL: SSL 2.0 has security weaknesses and is hardly used today; SSL 3.0 is universally supported; and finally the Transport Layer Security (TLS), which is an improvement on SSL 3.0, has been adopted as an Internet standard and is supported by almost all recent software.

Encryption protects data from unauthorized use by converting it to an apparently meaningless form before transmission. The data is encrypted by one side (the client or the server), transmitted, decrypted by the other side, then processed.
Source authentication is a method of verifying the data sender's identity. The first time a browser or other client attempts to communicate with a Web server over an insecure connection, the server presents the client with a set of credentials in the form of a **certificate**.

Certificates are issued and validated by trusted authorities known as **certification authorities (CAs)**. A certificate represents the public-key identity of a person. It is a signed document that says: *I certify that the public key in this document belongs to the entity named in this document. Signed (certificate authority).* Well-known CAs include Verisign, Entrust, and Thawte. Note that the certificates used with SSL/TLS today are X.509 certificates. *Data integrity* refers to means of ensuring that data has not been modified in transit.

The SSL connections act like sockets connected by TCP. Therefore, you can think of SSL connections as secure TCP connections since the place for SSL in the protocol stack is right above TCP and below the application layer as shown in Figure 3.8. It is important to note, however, that SSL doesn't support some of the TCP features such as out-of-band data. The SSL *full* handshake protocol is illustrated in Figure 3.9. It shows the sequences of messages exchanged during the SSL handshake.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

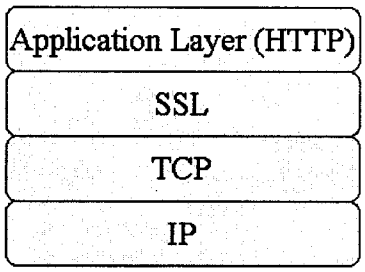


Figure 3.8: SSL and the TCP/IP protocol stack

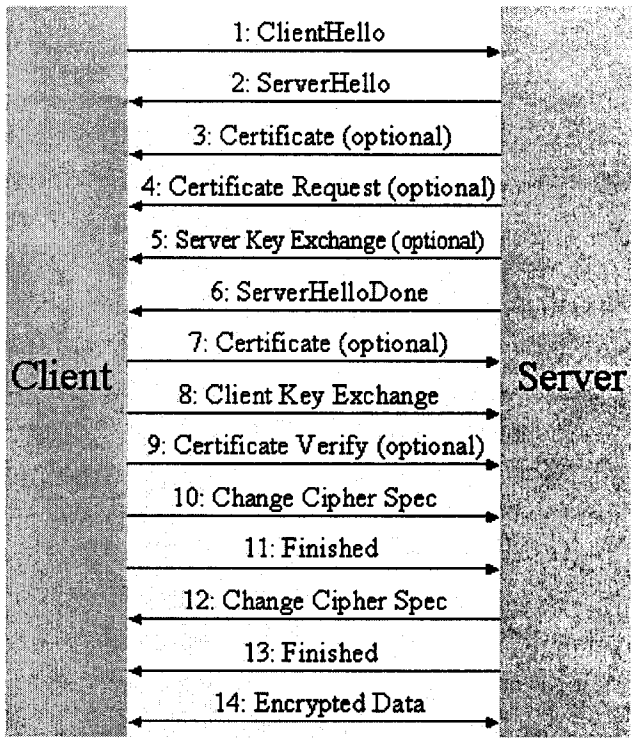


Figure 3.9: SSL handshake protocol

Among the features of SSL that have made it the standard vehicle for secure e-commerce transactions is its support for negotiable encryption and authentication algorithms. The designers of SSL realized that not all parties will use the same client software and consequently not all clients will include any particular encryption algorithm. The same is true for servers. The client and server at the two ends of a connection negotiate the encryption and decryption algorithms (cipher suites) during their initial handshake. It may turn out that they do not have sufficient algorithms in common, in which case the connection attempt will fail.

Note that while SSL allows both the client and the server to authenticate each other, typically only the server is authenticated in the SSL layer. Clients are customarily authenticated in the application layer, through the use of passwords sent over an SSL-protected channel. This pattern is common in banking, stock trading, and other secure Web applications.

Incorporating SSL into existing client/server applications to make them secure can be easily done using a few lines of JSSE code. The lines highlighted in **bold** in the following example show the code necessary to make a server secure:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

```
import java.io.*;
import javax.net.ssl.*;

public class Server
{
  int port = portNumber;
  SSLServerSocket server;
  try
  {
    SSLServerSocketFactory factory =
      (SSLServerSocketFactory) SSLServerSocketFactory.getDefault();
    server = (SSLServerSocket) factory.createServerSocket(portNumber);
    SSLSocket client = (SSLSocket)
        server.accept();

    // Create input and output streams as usual
    // send secure messages to client through the output stream
    // receive secure messages from client through the input stream
  }
  catch(Exception e)  {  }
}
```

The lines highlighted in **bold** in the following example show the code necessary to make a client secure:

```
import java.io.*;
import javax.net.ssl.*;

public class Client
{
  try
  {
    SSLSocketFactory factory =
      (SSLSocketFactory) SSLSocketFactory.getDefault();
    server = (SSLServerSocket) factory.createServerSocket(portNumber);
    SSLSocket client = (SSLSOcket) factory.createSocket(serverHost, port);

    // Create input and output streams as usual
    // send secure messages to server through the output stream
    // receive secure messages from server through the input stream
  }
```


Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

```
    catch(Exception e)  {  }
}
```

With the implementation of SSL in messenger system, we can believe that

- No error message will be delivered,
- No message will be delivered to an un-authorized user,
- No message can be attacked by a third party.

3.5 Conclusions:

This chapter provides details on the communication infrastructure used at our mammography consultation system. Three channels are found necessary: The Doctors XML Instant Messages Channel, The Image File Transfer Channel, and The SSL Protection Channel for both Instant Messages and Image Files. The design details for programming these channels in Java are provided for this purpose.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Chapter 4

Developing Lightweight Image Protection Techniques for Ubiquitous Environment

4.1 Lightweight Encryption:

When one begins to think about security and P2P networks, and in particular, ad-hoc P2P ubiquitous networks with no real centralization, one must take a leap from the accepted, in place, on-the-Internet, security practices into the unknown. Ubiquitous technology has exploded in healthcare because of its ability to improve the efficiency and accuracy of information exchange. Ubiquitous, mobile and pervasive environments allow caregivers and administrative staff to use mobile carts, Laptop PCs, handheld PCs, 3G Mobile Phones, PocketPCs and PDAs anywhere, anytime to access seamlessly all of media existing on the healthcare system or the internet.

However, security is the primary concern for the healthcare system due to the value of healthcare demographic data to a malicious hacker or due to the theft of such ubiquitous hand held devices. Special, reconfigurable and reliable security is particularly needed for the storage and transmission of digital medical images since medical data are image intensive. Unfortunately, the classical techniques for data security are not appropriate for the use in the current ubiquitous devices. Traditional encryption and decryption security approaches are computationally demanding causing a severe problem for ubiquitous devices, where power consumption needs to be reduced as much as possible as well as the optimal use of its tiny memory. Moreover, the image data size are usually very large and needs to be processed in real time. Encryption algorithms with high security will put great burden on storage space requirements and increase latency especially if such images were compressed. Actually image data security differs largely from the traditional textual data security where their information rate is very high, but the information value is quite low. Thus to break encrypted image data becomes much more expensive than to buy the original data [Yi, et.al., 2001]. For these reasons, the US National Institute of Standards and Technology (AES), US Government Federal Information Processing Standards (FIPS), the European Union (NESSIE), and the 3rd Generation Partnership Project (3GPP), IEEE (the IEEE 802.11 standard) and the International Multimedia Telecommunications Consortium (IMTC) have all issued calls for new *lightweight* encryption algorithms that satisfy higher security for ubiquitous environments. In information technology, the term *lightweight* is sometimes applied to a program, protocol, algorithm, device, or anything that is relatively simpler or faster or that has fewer parts than something else. In this chapter we developed an innovative lightweight encryption algorithm based on a dynamic stream cipher. This algorithm can be used besides the secure protocols (e.g SSL) used for

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

transmitting the medical images. It is very important for protecting medical images stored on ubiquitous devices. The secrecy of our developed algorithm has been tested according to the FIPS-140-1 standard. The comparison with other traditional stream ciphers reveals our algorithm superiority.

4.2 Traditional Approaches to Image Protection:

A huge amount of research work has been done in the area of image security and protection especially for the Web media. Various multimedia protection technologies have also appeared in[Stajano, 2002]. We can summarize these research attempts as follows:

- ***Heavyweight Cryptographic Approach***: Many perfect cryptographic ciphers have been established and applied widely since 1970s. But most conventional ciphers cannot be directly used to encrypt digital image for ubiquitous/wireless systems because their encryption speed is not fast enough, especially when they are realized by software [Raghunathan, et.al., 2003]. Such cryptographic primitives are often called heavyweight or JCE (Java Cryptographic Extension http://java.sun.com/products/jce/). Most of such primitives are based on public-key encryption algorithms, designed for reliable data services. Often such primitives cause severe error propagation and imply a loss in traffic capacity in exchange for privacy when used for ubiquitous environments [Juul, 2002]. Compared with secret-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data such as images. However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol. Moreover, public key encryption requires a special infrastructure for the ubiquitous environment (eg. PKI), an expensive solution which lets most venders to rely on secret-key encryption. Even for the traditional secret-key encryption we facing many difficulties especially if they implements *block ciphers (e.g. DES)*. There are many variants of the traditional DES algorithm designed for ubiquitous environments (e.g. MISTY, Camellia, RC6, SAFER, and Kasumi, Rijndael, Twofish, and FEA-M) are proved to use many computationally intensive operations and run at several rounds. For some rounds still there is no perfect secrecy when blocks are examined on the viewpoint of pseudo randomness [Courtois, Pieprzyk, 2002]. Furthermore, all block cipher algorithms adhere to the strict avalanche criterion (SAC) which states that an average of one-half of the output bits should change whenever a single input bit is complemented. Thus, block algorithms propagate bit errors; that is, a single bit error in an encrypted block will cause multiple bit errors in the decrypted block. On the other hand, modern stream cipher algorithms offer an improved performance compared with block ciphers (typically a factor 4-5 if measured in speed). However, the security of stream ciphers is not as well understood as for block ciphers. Most proposed stream ciphers such as RC4 (used for WEP), A5/1 (used for GSM), have security weaknesses [Fluhrer, et.al., 2001]. In the recent years, new stream based

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

algorithms such as E0, SOBER-t16 and SOBER-t32, claim to offer better security. The main other advantage of stream ciphers over the block ciphers is that they do not have error propagation, but do propagate synchronization errors caused by packet losses. That is, if the decryptor loses synchronization with the encryptor, all the recovered bits after the synchronization error will be "garbled" until synchronization is restored.

- ***Image Coding Approach:*** Discrete wavelet transform (as used in JPEG2000) has proven to be far better than the DCT (as used in JPEG or MPEG) as well as the FFT (as used in OFDM). The FFT suffers from known drawbacks (e.g. no time information). Solution to such drawbacks in the Fourier analysis techniques may be introduced by using a multi-resolution analysis. The wavelet transform, on the other hand, uses basis functions that are generated from a compactly supported mother wavelet by means of dilations and translations. Not just any function makes a wavelet, there are two conditions to be met: admissibility and regularity and many problems to be solved (e.g orthogonality, efficiency). Moreover, traditional DWT algorithms suffers also from having a complex procedure to determine the next subband with a better distortion rate and smaller number of coefficients as well as having complex quantizers and entropy coders. Many new variations of the basic DWT technique (e.g EZT, LTW) tried to solve the above problems and provide simpler algorithms for image and video coding. [Shapiro, 1993], but still they prove not be secure enough from strict cryptographic viewpoint although they offer joint compression-encryption methods [Uservitch, 2001].
- ***Digital Watermarking Approach:*** Encryption or Image Coding is often insufficient to protect digital contents [Wu, Kuo, 2001]. Basically there is a need for complementary methods and tools to protect ones intellectual property rights. It has been initiated by the relatively new research field of "digital watermarking". Image watermarking is commonly applied in the spatial and transform domains to achieve robust protection using techniques like LSB, Binary Mask, DCT, etc. There are a large variety of such watermarking schemes that address many different application scenarios: copyright protection, data authentication, ownership identification etc. A great deal of research has been devoted to the study of different *means* of labeling data and to the development of *robust* watermarking techniques within the Web environment. Obviously, watermarking will add increasing complexity to any security system and can only implemented as an embedded property to ubiquitous devices.
- ***XML Encryption Approach:*** The very features that make XML so powerful for business transactions (e.g., Web-ready nature, interoperability) provide both challenges and opportunities for the application of encryption and digital signature operations to XML-encoded data [Mactaggart, 2003]. W3C introduced recently two new security initiatives designed to both account for and take advantage of the special nature of XML data (XML Signature and XML Encryption). Together they will let Web services send and receive sensitive data confidentially. XML Encryption will be able to encrypt digital content such as GIF images, Scalable Vector Graphics (SVG) images, XML fragments or Cascading Style Sheets (CSS). It will have the ability to encrypt parts

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

of an XML document while leaving other parts open to encrypt the XML itself, or super-encrypt data. However, describing image raw contents as a structured collection of resources in a standard manner requires: **(1)** a standard and flexible metadata format; **(2)** a standard way to aggregate multiple resources of various types; and **(3)** a standard way to express structural relationships within the resource collection. Currently, only ad hoc metadata schemes are employed in several applications that are implemented using DOM. Only recently the XML consortium introduced the MPEG-21 standard and its related technical elements (e.g DID, DIID, IPMP, REL, DIA) to establish a uniform and flexible multimedia data abstraction and interoperability schema for declaring/packaging multimedia digital items using XML. However, applying such framework is still only restricted to internet Web applications.

- ***Visual Cryptography Approach:*** Visual Cryptography is a relatively new branch in cryptography which uses graphical shares and a decryption process involving the human visual sense. It requires intensive computations to process the complex key especially for color images. The decrypted images generally suffer from very low resolution and contrast because of the added random noise to the shares [Naor, Shamir, 1997]. For this reason it is an impractical approach for ubiquitous applications which generally use very small and low resolution screens.

4.3 Lightweight Stream Ciphers: An Introduction:

Generally, a lightweight stream cipher generator utilizes shift registers. A suitable shift register for stream cipher applications must have large periods, large linear complexities and possess certain randomness properties [Colomb, 1967]. The use of clock-controlled linear shift-registers in keystream generators appears to be good way of achieving sequences with these properties. A *Linear Feedback Shift Register* (LFSR) is a basic mechanism for generating a sequence of binary bits. The register consists of a series of cells that are set by an initialization vector that is, most often, the secret key. The behaviour of the register is regulated by a clock and at each clocking instant, the contents of the cells of the register are shifted right by one position, and the XOR of a subset of the cell contents is placed in the leftmost cell. One bit of output is usually derived during this update procedure. LFSRs are fast and easy to implement in both hardware and software (Figure 4.1). With a judicious choice of *feedback taps* the sequences that are generated can have a good statistical appearance.

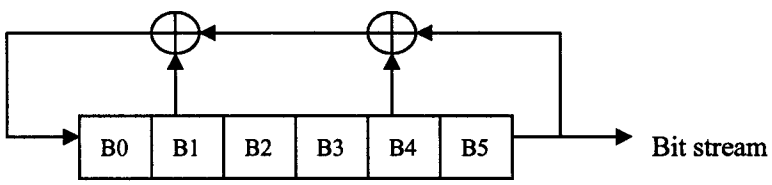


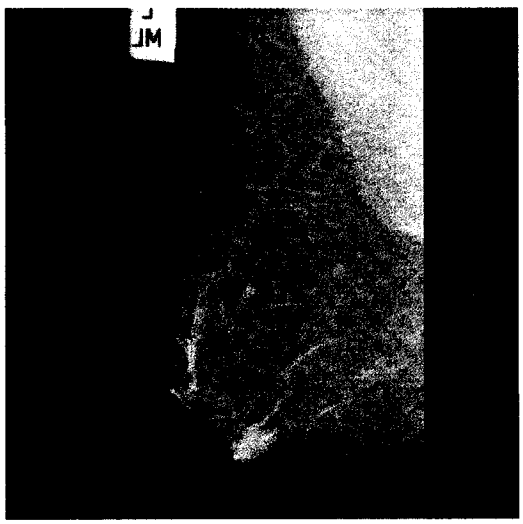
Figure 4.1: Linear Feedback Shift Register (LFSR)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

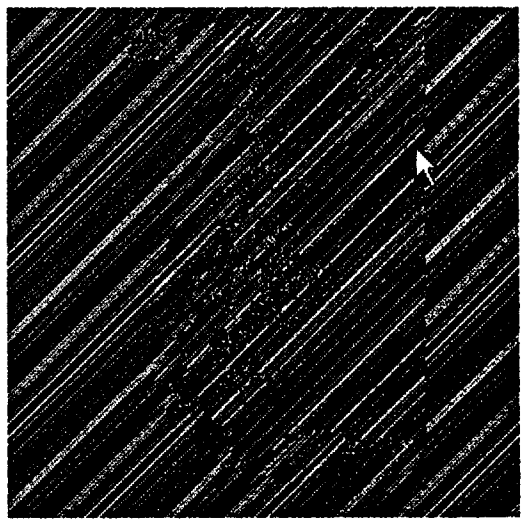
By properly selecting the tap positions on the LFSR, one can generate a pseudorandom or pseudo-noise (PN) sequence of maximal length (m-sequences). If we set the n possible shift register taps and initial state with n bits each, we can generate a large number of different maximal length PN sequences and start positions. If there are for example a LFSR with length n = 128 bits in the key to select taps, then the maximal length so of the keystream generated is= $2^{128} - 1 = 10^{38.4}$ bits. Indeed the length of the keystream is important as it impacts the length of time required to break the code. For example, if we assume that we are using a computer that can examine one billion keys per second we have table 4.1. If the length of keystream much smaller than the bit string of an image, some pattern will visually appear in the encrypted image. As illustrated in figure 4.2(b), a short keystream generated from an 8-bit key appears periodically, while 16 bit and 32 bit keys have visually random results.

Length of key bits	Number of combinations possible	Time required to break the cipher
1	2	$2*10^{-9}$ second
6	64	$6.4*10^{-8}$ second
24	$16.7*10^{5}$	0.167 second
40	$1.1*10^{12}$	18.16 minutes
56	$7.2*10^{16}$	2.286 years
128	$3.4*10^{38}$	$1.08*10^{22}$ years

Table 4.1: Estimated Time to break the cipher using Various LFSR lengths.

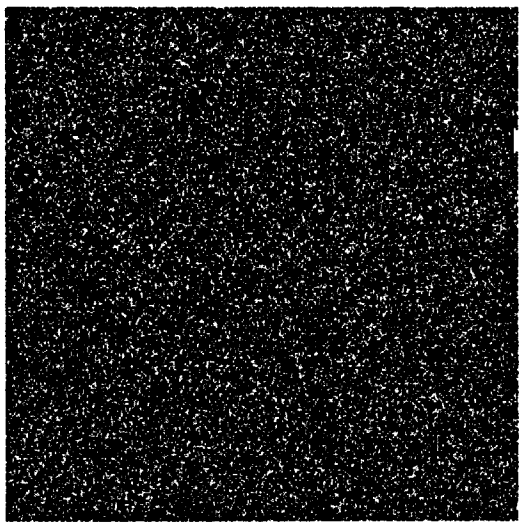


(a) Original image

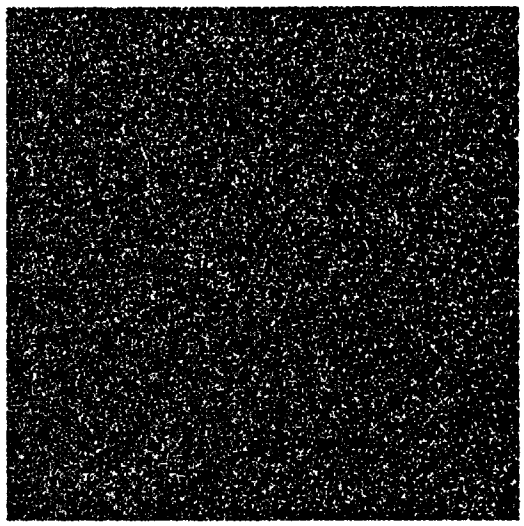


(b) Encrypted with key bits length=8, connections=5

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



(c) Encrypted with key bits length=16, connections=5



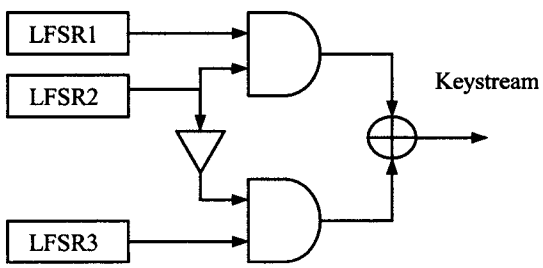
(d) Encrypted with key bits length=32, connections=5

Figure 4.2: Encryption examples of LFSR with different keystream length.

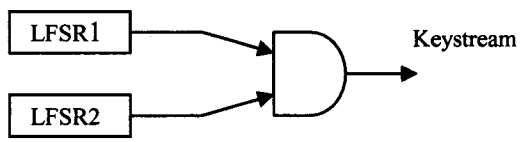
4.4 Traditional Lightweight Stream Ciphers:

The classical lightweight stream ciphers are generally based on static structures of nonlinear shift registers. According to Schneier [Schneier, 2000] stream ciphers provides low security when they are based solely on linear shift registers with exclusive-OR combiners. For this reason, many classical attempts have made to replace the weak XOR combiner with other nonlinear combiners. Figure 4.2 list some notable nonlinear combiners (e.g. Geffe, Hadamard, JK FF, A5/1,2,3, FCSR, and Hybriding FCSR and LFSRs) found in the literature which can work with ubiquitous environments [Stajano, 2002]. Mostly such designs have been used to provide security for the mobile short message system (SMS).

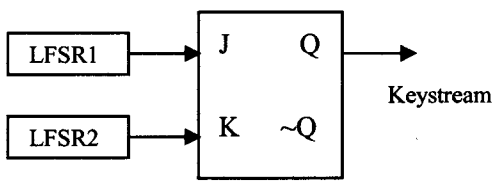
(a) Geffe combiner



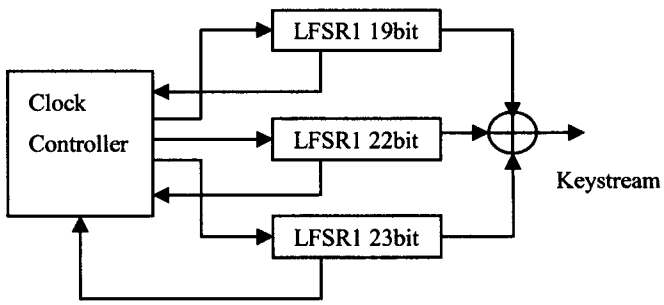
(b) Hadamard Combiner



(c) JK FF Combiner

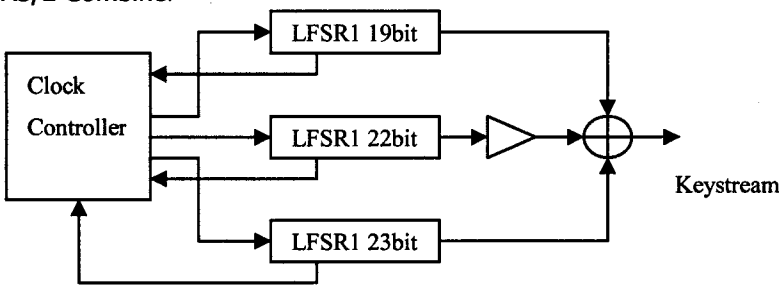


(d) A5/1 Combiner

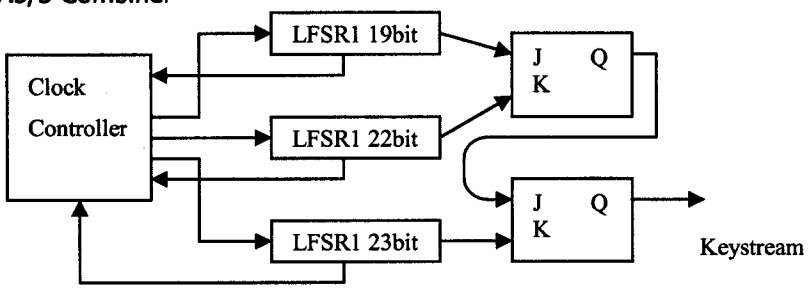


Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

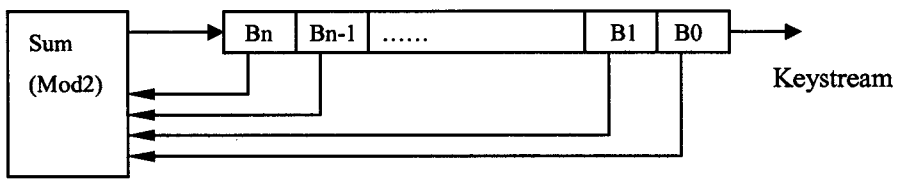
(e) A5/2 Combiner



(f) A5/3 Combiner



(g) FCSR Combiner



(h) Hybrid Combiner (FCSR &LFSRs)

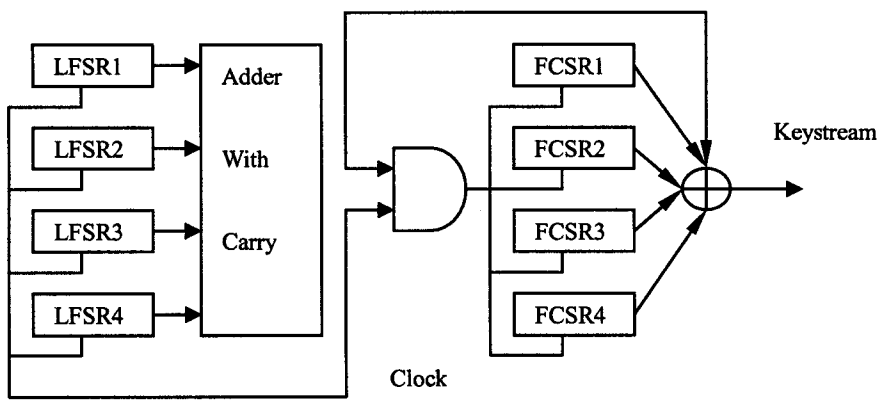


Figure 4.3: Notable Nonlinear Combiners.

Such designs prove to be practical and provide higher security because of the nonlinearity of the generated keystream with substantial long internal state as well as the good keystream randomness features. Images represent large data and requires very effective

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

and high performance encryption algorithm if compared to the traditional text mode encryption. Moreover, these designs have a static structure and the only way to reprogram them is to manually change the initial keys utilized by their basic LFSRs or FCSRs (See Figure 4.4).

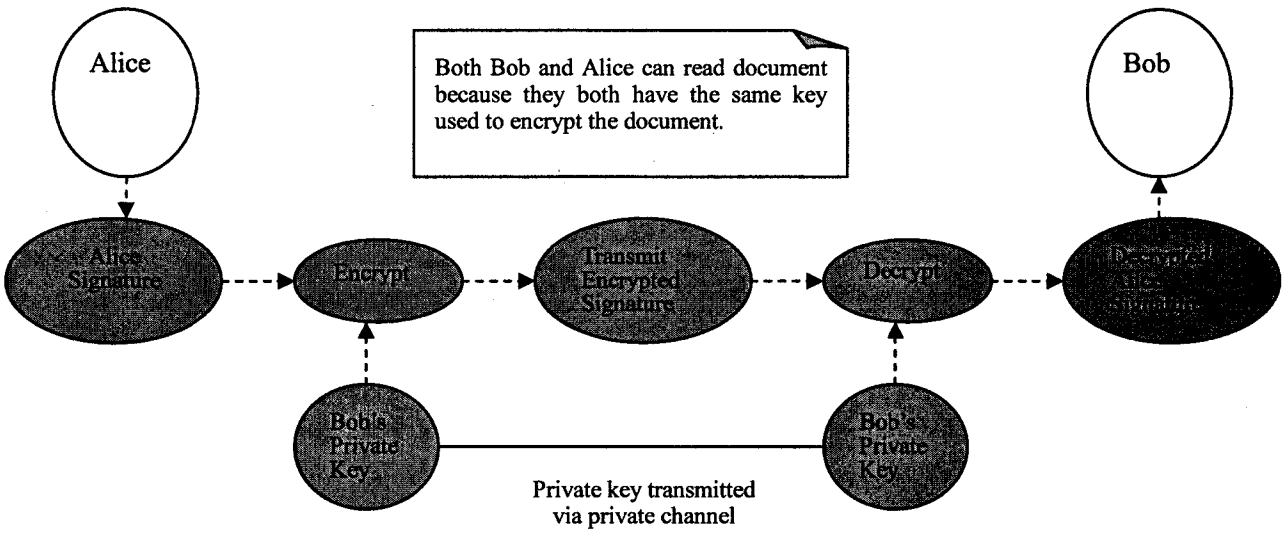


Figure 4.4 Classical Lightweight Stream Ciphers requires frequent rekeying.

4.5 Design of a Dynamically Controlled Nonlinear Lightweight Stream Cipher Combiner

Frequently manually rekeying such designs is not practical at the healthcare environment where workers can rarely meet in a short time. Indeed, a fast rekeying or a dynamically reconfigurable stream cipher combiner will make the job of the cryptanalyst much harder and can never let him/her to see very much plain image data encrypted with any one key or one particular design keystream generator. In this direction we are proposing a dynamically controlled nonlinear combiner (or LFSRs Controlled by another LFSR (LCL)) which can take advantage of some of the notable combiners and alter dynamically the way the keystream is generated according to the value of some the bits of one of its contributing LFSRs or LCSRs. For a practical realization we decided to have eight LFSRs (or LCSRs) and to let the eighth LFSR decides which combiner to be selected at each clock iteration (see Figure 4.5). The eighth LFSR will decide to use one of the five notable combiners to combine the first seven LFSRs at each clock cycle. We used the last three bit of LFSR #8 to define the identifier number (ID) of the selected combiner. Furthermore, in order to produce higher keystream cycles, we considered that the length of LFSR1~LFSR7 should satisfy the following conditions: gcd (L1, L2, L3) = 1;

gcd (L4, L5, L6, L7) = 1;

Figure 4.6 describes the dynamic combiner algorithm.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

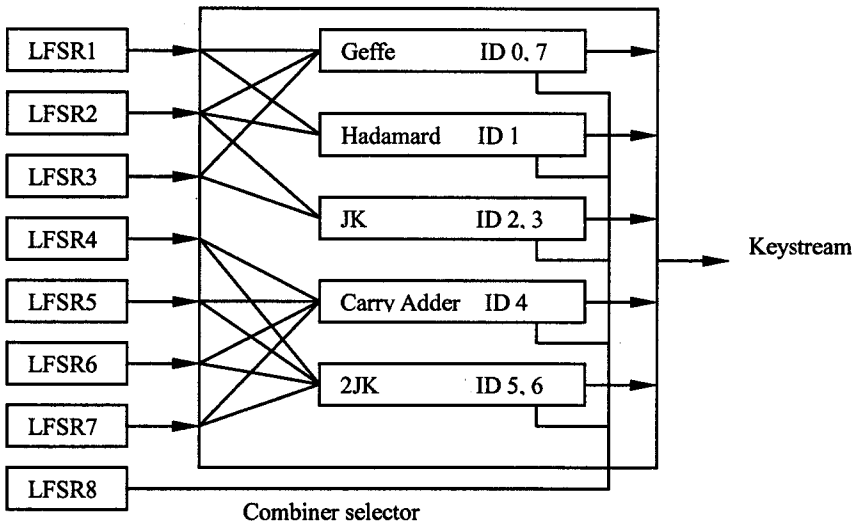


Figure 4.5: Dynamically Reconfigurable Combiner.

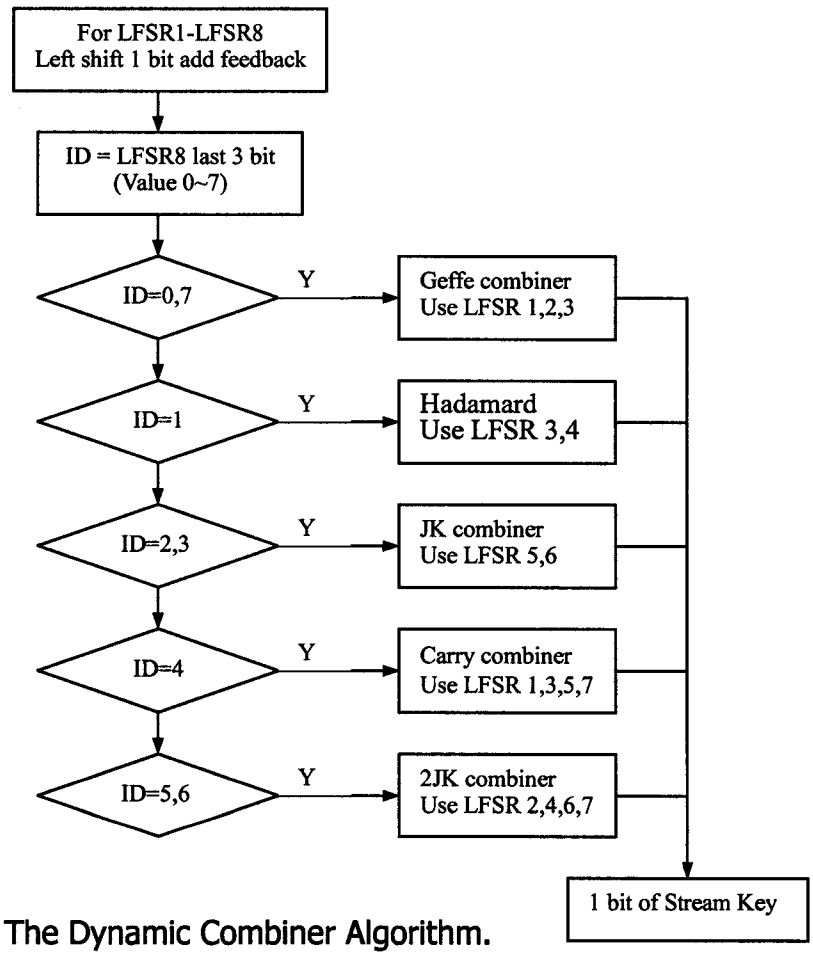


Figure 4.6: The Dynamic Combiner Algorithm.

For the purpose of evaluating the security strength of the various image protection combiners, we used the NIST FIBS 140-1 standard measures [FIPS 140-1, 1994]. The FIBS

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

standard includes measures that can test the randomness nature of the ciphered image data. It includes four measures: Monobit Test, Poker Test, Runs Test and Long Run Test. For this purpose, we encrypted five medical images plus one control image which is completely black (figure 4.7). We took the first 20,000 bit sample of each ciphered image data for the purpose of our evaluation.

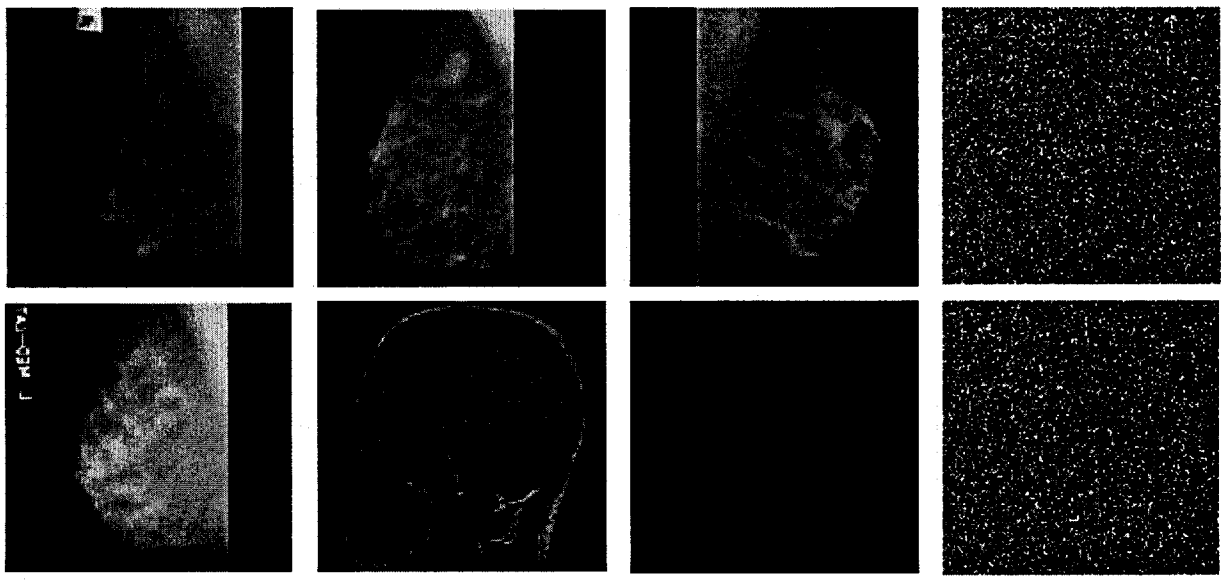


Figure 4.7: Test Images and encrypted images for the first 2 mammograms.

The monobit test counts the number of ones (X) in the 20,000 bit sample. The test is passed if 9,654 < X < 10,346. The poker test divides the 20,000 bit stream into 5,000 contiguous 4 bit segments. Count and store the number of occurrences of each of the 16 possible 4 bit values. Denote $f(i)$ as the number of each 4 bit value i where 0 <= i <= 15. Then, evaluate the following:

$$X = \frac{16}{5000} \times \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000$$

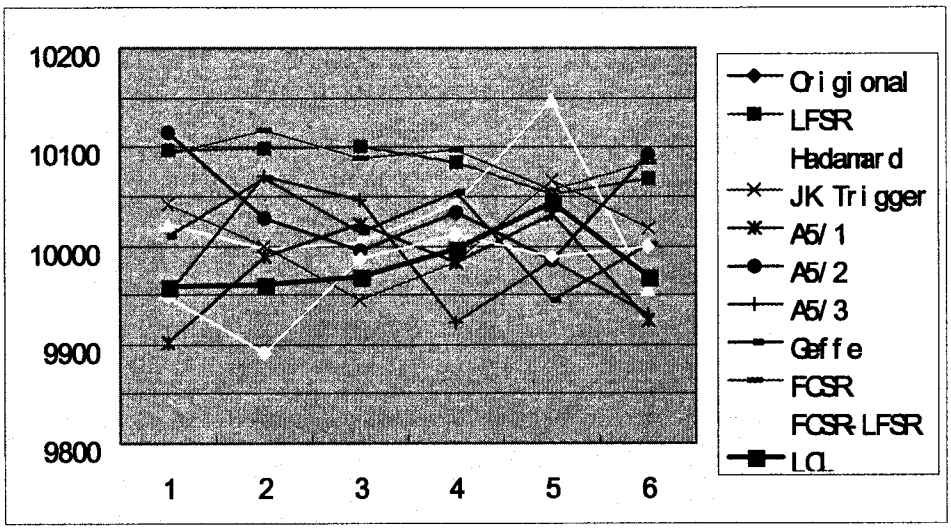
The poker test is passed if 1.03 < X < 57.4.

A run test identify the maximal sequence of consecutive bits of either all ones or all zeros. The test is passed if the number of runs that occur (of lengths 1 through 6) is each within the corresponding interval specified below. This must hold for both the zeros and ones.

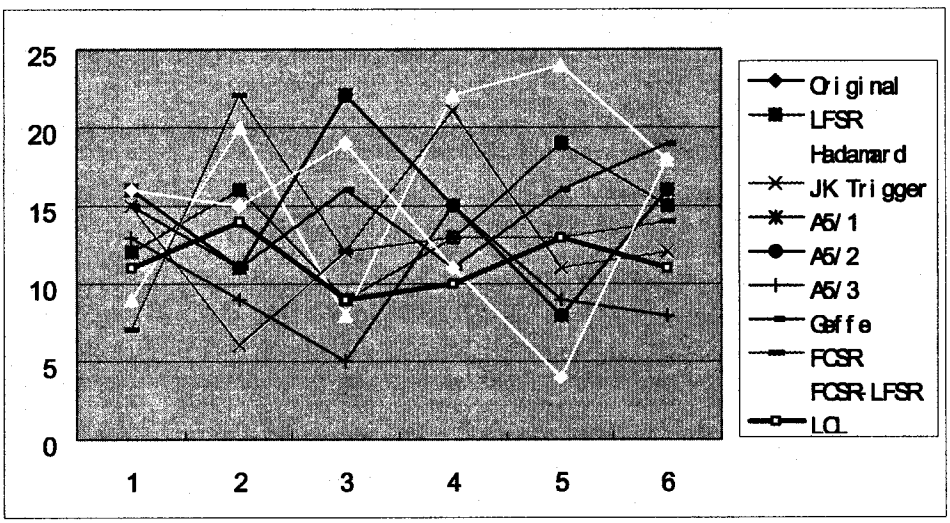
1	2,267–2,733	2	1,079-1,421
3	502 – 748	4	223 – 402
5	90 – 223	6	90 – 223

A long run test identify the availability of runs of length 34 or more (of either zeros or ones). The test is passed if no such long runs available in the sample. Figure 4.8 compare the dynamic combiner LCL with the other notable combiners as well as with original binary data image before encryption.

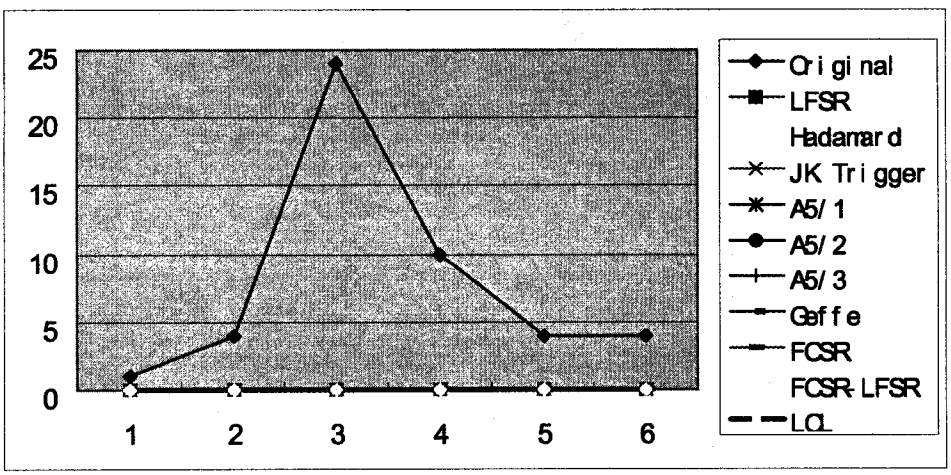
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



(a) Monobit Test Comparison.



(b) Poker Test



(c) Long Run Test

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

0 runs	Original	LFSR	Hadamard	JK trigger	A5/1	A5/2	A5/3	Geffe	FCSR	FCSR-LFSR	LCL
1	1337	2506	2465	2401	2457	2481	2473	2488	2547	2453	2475
2	517	1215	1291	1269	1217	1224	1253	1292	1260	1238	1254
3	339	635	624	602	641	597	606	612	630	627	622
4	193	327	321	306	341	364	317	322	297	310	329
5	108	146	158	177	153	137	146	165	151	175	157
6+	80	151	144	163	158	164	162	135	146	174	156

(d) Zero Run test for the Left Fist Image.

1 runs	Original	LFSR	Hadamard	JK trigger	A5/1	A5/2	A5/3	Geffe	FCSR	FCSR-LFSR	LCL
1	1123	2464	2560	2441	2481	2459	2456	2444	2516	2511	2551
2	514	1235	1201	1209	1224	1216	1236	1343	1230	1249	1189
3	522	654	590	612	597	641	591	589	639	609	601
4	248	283	322	331	364	341	331	320	330	296	320
5	95	170	165	157	137	153	175	165	161	150	183
6+	73	173	166	167	164	158	167	152	156	163	148

(e) One Run Test for the Left Fist image.

Figure 4.8: Comparing the different Combiners.

Although all the combiners passed all the tests, the LCL dynamic combiner is still showing much better results as it always approaching the median of the intervals. This is indeed besides its reconfiguration ability which provides much better security from the cryptanalyst point of view.

4.6 Conclusions:

In the ubiquitous world nowadays, the security of digital images becomes more and more important since the storage of digital products on such handheld devices is subject to theft. Lightweight cryptography based on stream cipher combiners is studied as an alternative and a dynamic reconfigurable combiner has been designed to improve security over the classical combiners. There are many future enhancements to current system where we need to test other combiners such as *step generator*, the *cascade generator*, and the *shrinking generator*. The performance of our LCL needs to be carefully monitored on various ubiquitous devices and not only the two P4 Laptop computers originally tested on.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Chapter 5

Conclusions and future research

Thesis Summary and Findings

Our thesis attempts to design and develop a prototype for mammography image consultation that can work within a ubiquitous environment. It is important to note that the work on mammogram images differs largely from other type of images. Several factors affect the proper segmentation of mammograms: Mammograms contain low signal to noise ratio (low contrast) and a complicated structured background. Thus mammograms are complex images which show many variations of both normal and abnormal breast tissue. Indeed, screening mammography checks asymptomatic women for signs of breast disease, particularly breast cancer. Diagnostic mammography is used to assess women who have clinical symptoms of breast disease or an abnormality detected on a screening mammogram. As a screening and diagnostic tool, mammography is one of the best ways to detect breast cancer, as mammograms can show cancers that are too small to be felt during physical examination. As the success of breast cancer treatment is improved if a cancer is detected early, using mammography to detect early cancer is very important.

The thesis includes the following chapters:

Chapter 1: Critically reviewed the diverse approaches on Computer-Aided Mammography. The review focused on techniques of image segmentation and the attempts to diagnose abnormalities in breast X-rays.

Chapter 2: This chapter focuses on the first stage in image segmentation, that is edge detection. The first part of this chapter explores the affectivity of the various traditional techniques based on convolution operators (e.g. Sobol, Pretwitt, Canny) for mammography edge detection. The second part of this chapter tries to enhance the results obtained via the traditional techniques by hybriding some of them. The hybriding technique is called in our thesis as Pipelined Operators. In this direction we proposed four pipelined operators which contributes to edge enhancement as wéll as abnormalities rendering through the introduction of an additional coloring mechanism. Although the visualization pipelines represent in our view an advancement on the traditional techniques applied to mammograms, such pipelines expose healthcare users to further usage complexities. For this purpose we extended our research on edge detection to find a better single technique that can work smoothly within the healthcare system. In this direction, we developed in the third part of this chapter a novel technique for finding edges based on analyzing the dynamic and fuzzy nature of edges in mammograms. We called our developed method as

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

"Dynamic Fuzzy Classifier or the DFC". Comparison shows that the DFC has advantages far beyond simplicity: It is far better than any edge detection method that we came across in this research. The DFC method have been tested on two notable medical mammography image databases.

Chapter 3: This chapter developed an integral communication infrastructure that can work in a ubiquitous environment like the healthcare system. Three main channels have been identifies as vital for this infrastructure: The healthcare **instant messaging channel** (which we implemented according to W3C recommendation in XML to suite ubiquitous environments), the **image/file transfer channel** (which we implemented via the widely used TCP/IP protocol over the internet), and the **SSL image/file transfer protection protocol**. The combination of these three channels in one simple prototype work fantastically nice when tried by novice healthcare users. It provides simplicity and trust in securing the transferred messages and images/files. The heathcare users need only to plug their ubiquitous device and sends an instant message to their peers and the communication can proceeds afterwards smoothly.

Chapter 4: This chapter focuses on a different security issue that is highly important for the healthcare system where most of their ubiquitous devices are of the handheld type. It is highly likely that such devices are liable to theft or lost. Hence there is a great need to protect the stored data in such devices using a further security technique. Encryption is the most likely candidate to be used in this direction. However, due the nature of the ubiquitous devices, the use of the well-known heavyweight encryption techniques represents a great performance obstacle. In this direction we been looking to what is generally known as Lightweight encryption technique, which is mostly means stream ciphers. For this purpose, we implemented most of the notable lightweight stream ciphers used for mobile and ubiquitous environments (e.g. A5, Pless). Moreover, we decided to develop our own lightweight structure just to avoid the possibility of a hacker who may be well aware about the traditional lightweight structures. In this direction we developed a novel lightweight stream cipher that we called the "Dynamic Combiner". The secrecy power of our dynamic combiner is compared to the other traditional lightweight stream ciphers according to the international security standard **FIPS140-1**. The comparison proves our dynamic combiner is far better than the traditional lightweight ciphers. All the comparison experiments performed on mammogram images as well as any other file types.

Chapter 5: This chapter presents the summary, findings, and the future work of this research.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Future Research Directions:

We aim to extend our research in the following directions:

1. Extending our DFC method to be a full scale cancer diagnosis and segmentation. In this direction we would like to follow the lead of learning from the knowledge-base of previous cases as well as learning the structural characteristics of each type of Cancer or breast abnormalities [Zhang, Rosin, 2003, Zaiane, et.al., 2002].

2. We aim to use and extend our Dynamic Combiner for adding more security on the message and image transfer. For this purpose we aim to make our combiner self synchronous [Richter, 2002] and can recover from lost packets [Wu et.al. 2002] as well as to be more chaotic in the nature of the encrypted data [Li, Zheng, 2002].

3. We started some work on transferring the mammograms into wavelets and already you can find this entry in our system (see Figure 5.1). The use of wavelets is highly important to protect the intellectual identity of mammograms as well as to impose a highly effective compression technique [J.FIAIDHI, S.MOHAMMED, M.DIETZE, and S.JASSIM, 2003]. With wavelets we aimed to extend our research work to establish audio/video communication between healthcare workers [Perkins, 2003].

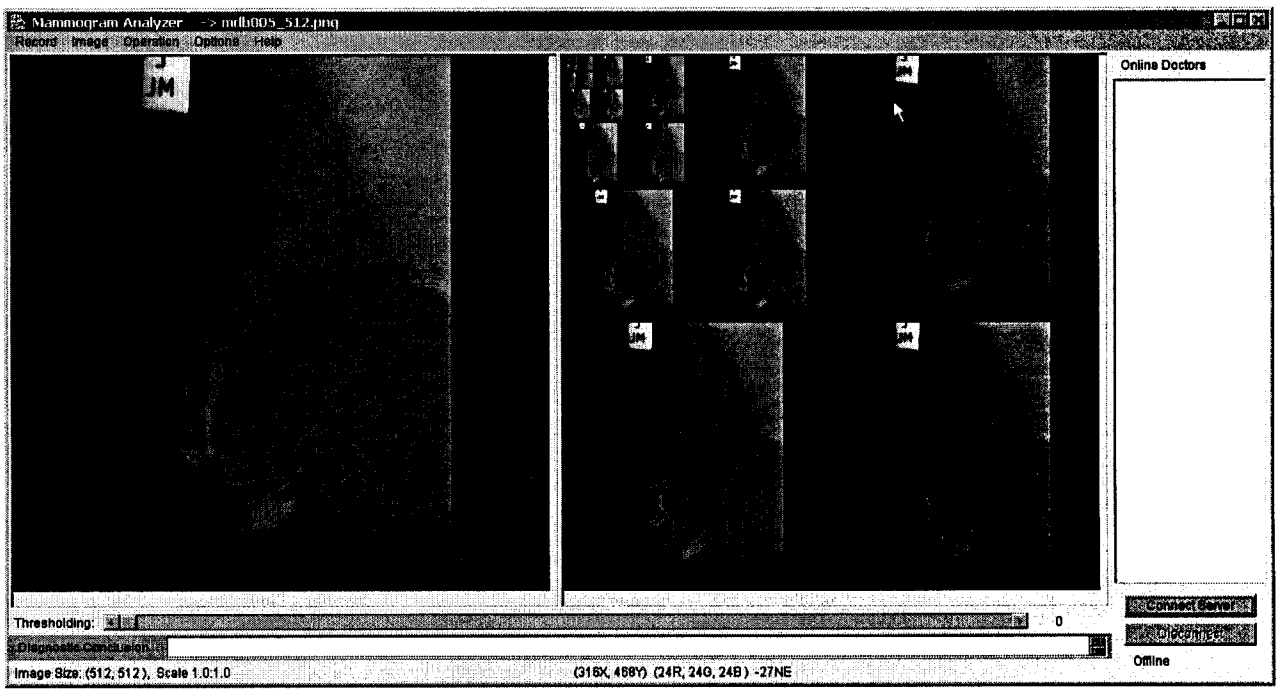


Figure 5.1: The use of wavelets in our system.

4. We would like modifying our work so to be effective for fully mobile environment. In this direction, we need to focus on J2ME instead of J2SE, WAP instead of SSL, and WEP instead of our lightweight protection, and JXTA instead of TCP/IP.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

References

[Antonie, 2001] Maria-Luiza Antonie, Osmar R. Za¨iane, and Alexandru Coman,Application of Data Mining Techniques for Medical Image Classification, International Workshop on Multimedia Data Mining MDM/KDD2001, San Francisco, August 26, 2001.

[Batchelor 1993] Bruce Batchelor and Frederick Waltz, Interactive Image Processing for Machine Vision, Springer Verlag, New York, 1993.

[Bazzani, et.al., 2000] A. BAZZANI, et al, SYSTEM FOR AUTOMATIC DETECTION OF CLUSTERED MICROCALCIFICATIONS IN DIGITAL MAMMOGRAMS, International Journal of Modern Physics C, Vol. 11, No. 5 (2000) 1–12

[Bovik AC, 1987] Bovik AC et al "The effect of median filtering on edge estimation and detection", *IEEE Trans. Pattern Anal. Machine Intell, vol PAMI-9, pp. 181-194, Mar 1987*

[Bovik, et.al., 1987] A.C. Bovik et al "The effect of median filtering on edge estimation and detection", *IEEE Trans. Pattern Anal. Machine Intell, vol PAMI-9, pp. 181-194, Mar 1987*

[Bredlie & Wood 2001] K. Bredlie and J. Wood, Recent Advances in Volume Visualization, Computer Graphics Forum, Vol 20, Issue 2, June 2001.

[Cafforio, et.al., 1997] C. CAFFORIO, E. DI SCIASCIO, C. GUARAGNELLA: G. PISCITELLI: "A Simple and Effective Edge Detector". Proc. of ICIAP'97, in Lectures Notes on Computer Science, A. Del Bimbo ed., vol.1310, pp. 134-141. Florence Sept. 1997.

[Colomb, 1967] S.W. Colomb, "Shift Register sequences", Holden-Day Publisher, 1967.

[Costa, Cesar, 2000] L. F. Costa and R. M. Cesar Junior , SHAPE ANALYSIS AND CLASSIFICATION: THEORY AND PRACTICE, CRC Press Book Series on Image Processing, 2000.

[Courtois, Pieprzyk, 2002] Nicolas T. Courtois and Josef Pieprzyk, Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, In Yuliang Zheng, editor, Advances in Cryptology (Asiacrypt2002), Lecture Notes in Computer Science. Springer-Verlag, 2002.

[Davies, Dance, 1992] Davies DH and Dance DR "Automatic computer detection of subtle calcifications in radiographically dense breasts", *Phys Med Biol 1992; 37:1385-1390.*

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

[Deite, et.al.l, 2001] H.M. Deitel, P.J. Deitel, T.R. Nieto, T.M. Lin, P.Sadhu, "*XML how to program*", Deitel & Associats Inc, 2001.

[De Parades, 1993] De Parades E,"Radiographic breast anatomy: radiologic signs of breast cancer", *Syllabus: 79th Scientific Assembly of the Radiological Society of North America, 1993, pp 35-46.*

[Elvins, 1992] T. Elvins, Survey of Algorithms for Volume Visualization, Computer Graphics, 26:3, pp194-201, August 1992.

[Fiaidhi, et.al., 2003] J. Fiaidhi, S. Mohammed, M. Dietze, and S. Jassim, Intellectual Property Protection for Collaborative eLearning Systems, Int. Conference on Internet Computing, Las Vegas, USA, June 23-26, 2003.

[Fiaidhi, et.al., 2004] J. Fiaidhi, S. Mohammed and Lei Yang, "On an Integral Approach for Searching XML Documents in a Collaborative Environment", *Asian Journal of Information Technology* 3 (1): 56-68, 2004, http://www.gracepublication.org/ajit/3(1)2004.htm;

[FIPS 140-1, 1994] FIPS 140-1 Specifications, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, http://www.itl.nist.gov/fipspubs/fip140-1.htm, NIST,1994 January 11

[Fluhrer, et.al., 2001] S. Fluhrer, I. Mantin and A. Shamir,"Weaknesses in the key scheduling algorithm of RC4", *Selected Areas in Cryptography - SAC2001*, Toronto, Canada, Aug. 2001, Workshop Record, pp. 3-25.

[Giger, 1993] Giger ML "Computer -aided diagnosis", *Syllabus: 79th Scientific Assembly of the Radiological Society of North America, 1993, pp 283-298.*

[Gonzalez, Woods 2002] R. Gonzalez and R. Woods, Digital Image Processing,2nd Edition, Addison-Wesley, 2002.

[Guillemet, 1996] Guillemet H, Benali H, et al "Detection and characterization of micro calcifications in digital mammography", Third International Workshop on Digital Mammography, Chicago June 1996.

[Halls, 2003] Steven B. Halls, MD http://www.halls.md/breast/density.htm, Nov.10, 2003.

[Hingham, et.al., 1996] R.P. Hingham, J.M. Brady et al "A quantitative feature to aid diagnosis in mammography" *Third International Workshop on Digital Mammography, Chicago June 1996.*

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

[Holland, 1982] Holland T et al "So-called interval cancers of the breast: pathologic and radiographic analysis", Cancer 1982; 49:2527-2533.

[Jenkin, Dymond, 2002] M. Jenkin, and P. Dymond, Secure communication between lightweight computing devices over the internet, 35th Annual Hawaii Int. Conf. on System Sciences (HICSS'02)-addendum, Jan. 07 - 10, 2002

[Juul, 2002] Niels Christian Juul, Security Issues in Mobile Commerce using WAP, 15th Bled Electronic Commerce Conf.: e-Reality: Constructing the e-Economy, Bled, Slovenia, June 17 - 19, 2002. http://www.bsa.org/policy/encryption/cryptographers.html

[Kuhlmann F, 1981] Kuhlmann F and Wise GL "On second moment properties of median filtered sequences of independent data", *IEEE Trans. Commun., vol. COM-29, pp. 1374-1379, 1981*

[Lai S, 1989] Lai S et al "On techniques for detecting circumscribed masses in mammograms", *IEEE Trans. on Medical Imaging, vol.8, no. 4, pp. 377-386, Dec. 1989*

[Liang, 2003] Lily Rui Liang, Carl G. Looney, "Competitive Fuzzy Edge Detection", International Journal of Applied Soft Computing, Volume 3, Issue 2, pp. 123--137, September, 2003.

[Li, Zheng, 2002] Shujun Li, Xuan Zheng, Cryptanalysis of a Chaotic Image Encryption Method (2002) Proceedings of 2002 IEEE International Symposium on Circuits and Systems (ISCAS 2002), vol. II

[Looney, 2000] C.G. Looney, Nonlinear rule-based convolution for refocusing, Real Time Imaging 6 (2000) 29–37.

[Looney, 2002] C.G. Looney, Radial basis functional link nets and fuzzy reasoning, Neurocomputing 48 (1–4) (2002) 489–509.

[Looney, 1997] C.G. Looney, Pattern Recognition Using Neural Networks, Oxford University Press, New York, 1997.

[Mactaggart, 2003] Murdoch Mactaggart, "Enabling XML Security",IBM Technical report, Sept 21,2003, http://www106.ibm.com/developerworks/security/library/s-xmlsec.html

[Mahmoud 1996] Sockets programming in Java: A tutorial, Qusay H. Mahmoud, JavaWorld Online Journal, December 1996,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

http://www.javaworld.com/javaworld/jw-12-1996/jw-12-sockets_p.html

[Maxwell, Brubaker, 2003] B. A. Maxwell and S. J. Brubaker Texture Edge Detection Using the Compass Operator, British Machine Vision Conference 2003.

[McLeod, et.al., 1996] McLeod G., Parkin G. et al "Automatic detection of clustered microcalcifications using wavelets", *Third International Workshop on Digital Mammography, Chicago June 1996.*

[Meersman, et.al., 1996] Meersman D, Scheunders P et al "Detection of microcalcifications using neural networks", *Third International Workshop on Digital Mammography, Chicago June 1996.*

[Mendonca, et.al., 1996] Mendonca Brago Neto U, Siqueira Neto W et al "Mammographic calcification detection by mathematical morphology methods ", *Third International Workshop on Digital Mammography, Chicago* June 1996.

[MIAS] Mammographic Image Analysis Society (MIAS) http://www.wiau.man.ac.uk/services/MIAS/MIASweb.html.

[Mohammed, et.al., 2003(a)] Sabah Mohammed, Jinan Fiaidhi and Lei Yang, *Morphological Analysis of Mammograms Using Visualization Pipelines*, Pakistan Journal of Information & Technology , 2 (2): 178-190, 2003, http://www.ansinet.net/PJIT_currentissues.asp;

[Mohammed, et.al., 2003(b)] Sabah Mohammed, Jinan Fiaidhi and L. Yang, *Developing an A5 Image Cryptographic System for the 3G GSM Systems Based on Chaotic Image Cryptography*, Asian Journal of Information Technology 2 (4): 332-345, 2003, http://www.gracepublication.org/ajit/2(4)2003.htm;

[Mohammed, et.al., 2004(a)] Sabah Mohammed, Lei Yang and Jinan Fiaidhi, "A Dynamic Fuzzy Classifier for Detecting Abnormalities in Mammograms", Accepted for presentation at the *Canadian Conference on Computer and Robot Vision* (CRV2004), May 17-19, 2004, University of Western Ontario, Canada,

[Mohammed, et.al., 2004(b)] Sabah Mohammed, Jinan Fiaidhi and Lei Yang, "Developing Multitier Lightweight Techniques for Protecting Medical Images within Ubiquitous Environments", Accepted for presentation at the 2nd annual conference on Communication Networks and Services (CNSR 2004), Fredericton, N.B., Canada, May 19-21, 2004

[Mohammed, etal., 2004(c)] Sabah Mohammed, Jinan Fiaidhi and Lei Yang, chapter "The

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Roadmap for Recognizing Regions of Interest in Medical Images" at John Wiley & Sons book entitled "Computer Aided Intelligent Recognition Techniques and Applications" edited by M. Sarfraz to appear in June 2004.

[Muir BB, 1983] Muir BB, lamb J et al "Microcalcification and its relationship to cancer of the breast: experience in a screening clinic", *Clinical Radiology* 1983; 149:193-200.

[Nagao, 1979] Nagao M et al "Edge preserving smoothing" *Comput.Graphics Image Processing, vol 9, pp394-407 1979*

[Naor, Shamir, 1997] M. Naor and A. Shamir, Visual Cryptography II: Improving the Contrast via the Cover Base,Vol. 1189 of Lecture Notes in Computer Science, Springer-Verlag,197-202, 1997.

[Neto, et.al., 1996] M. B. Neto U, W. N. Siqueira et al "Mammographic calcification detection by mathematical morphology methods ", *Third International Workshop on Digital Mammography, Chicago June 1996.*

[Netsch, 1996] T. Netsch, "Detection of micro calcification clusters in digital mammograms: A space scale approach", *Third International Workshop on Digital Mammography, Chicago June 1996.*

[Nodes TA, 1982] Nodes TA and Gallagher NC "Median filters: Some modifications and their properties", *IEEE Trans. Acoust., Speech Signal Processing, vol. ASSP-30, Oct 1982.*

[Parker 1997] Parker, J., R., "Algorithms for Image Processing and Computer Vision", Wiley Computer Publishing, 1997.

[Perkins, 2003] Colin Perkins, "RTP: Audio and Video for the Internet", Addison-Wesley, 2003. ISBN 0-672-32249-8

[Raghunathan, et.al., 2003] Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, and Jean-Jacques Quisquater, Securing Mobile Appliances: New Challenges for the System Designer, *IEEE Conference on Design, Automation, and Test in Europe (DATE03),* Munich, GERMANY, March 2003

[Richter, 2002] Graham Richter, Design, Analysis, Implementation and Comparison of Stream Cipher Algorithms, Technical Report No. 97192164, Department of Computer, Electrical and Electronic Engineering, University of Pretoria 10/03/02

[Rosin, 2002] P.L. Rosin, 'Thresholding for Change Detection', Computer Vision and Image

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Understanding, vol. 86, no. 2, pp. 79-95, 2002.

[Rosenfeld R, 1982]Rosenfeld R and Kak AC, "Digital Picture Processing " *New York Academic 1982*

[Russo, Rampon, 1992] F. Russo, G. Ramponi, Fuzzy operator for sharpening of noisy images, IEE Electron. Lett. 28 (1992) 1715–1717.

[Scher A, 1980] Scher A. et al "Some new image smoothing techniques", *IEEE trans. Syst., vol. SMC-10, no 3, pp 153-158, 1980*

[Schneier, 2000] Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc, 2000.

[Shapiro, 1993] J.M. Shapiro, "Embedded image coding using the zerotrees of wavelet coefficients", IEEE Tr. on Image Processing, Vol. 41, No. 12, , Dec. '93, 3445-3462.

[Sickles EA, 1982] Sickles EA, "Mammographic detectability of breast microcalcifications", *AJR 1982; 139:913-918.*

[Sickles EA, 1986] Sickles EA " Mammographic features of 300 consecutive non palpable breast cancers.", *AJR 1986; 146:662-663.*

[Stajano, 2002] F. Stajano, Security for Ubiquitous Computing, John Wiley and Sons Ltd, ISBN: -470-84493-0, 2002

[Tizhoosh, 1997] H.R. Tizhoosh, Fuzzy Image Processing, Springer Verlag, 1997.

[Undrill P, 1996] Undrill P, Gupta R et al "The use of texture analysis and boundary refinement to delineate suspicious masses in mammography" *SPIE Image Processing, Vol 2710, pp 301-310.*

[Undrill, et.al., 1996] P. Undrill, R. Gupta et al "The use of texture analysis and boundary refinement to delineate suspicious masses in mammography" *SPIE Image Processing, Vol 2710, pp 301-310.*

[Uservitch, 2001] B.E. Uservitch, Tutorial on Modern Lossy wavelet Image Compression, IEEE Signal Processing Magazine, September 2001.

[van der et.al., 2003] B.J. van der Zwaag, K. Slump, and L. Spaanenburg. On the analysis of neural networks for image processing. In V. Palade, R.J. Howlett, and L.C. Jain (eds.),

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proceedings of the Seventh International Conference on Knowledge-Based Intelligent Information & Engineering Systems (KES'2003, Oxford, UK, 3-5 Sept.), Part II, volume 2774 of *Springer LNCS/LNAI*, pages 950-958, 2003. Springer-Verlag.

[Wu, et.al., 2002] T. Wu, A. C. Miguel, E. A. Riskin, A. E. Mohr, R. E. Ladner, S. Hauck, "Protecting regions of interest in medical images in a lossy packet network," WORD FILE in Medical Imaging 2002: PACS and Integrated Medical Information Systems: Design and Evaluation, Eliot L. Siegel, H. K. Huang, Editors, Proceedings of SPIE Vol. 4685, 137-148 (2002).

[Wu, Kuo, 2001] C. P. Wu, C.-C. J. Kuo, Efficient multimedia encryption via entropy codec design, Security and Watermarking of Multimedia Contents III*Proceedings of SPIE* Vol. 4314, 22-25 January 2001California,USA.

[Yi et. al 2001] X. Yi, C.H. Tan, C.K. Siew and M.R. Syed, "Fast encryption for multimedia",IEEE Transactions on Consumer Electronics, vol. 47,101-107,Feb. 2001

[Yin FF, 1993]Yin FF, Giger ML et al "Comparison of bilateral-subtraction and single-image processing techniques in the omputerised detection of mammographic masses", *Investigative Radiology 1993; 28:473-481.*

[Yi, et.al., 2001] X. Yi, C.H. Tan, C.K. Siew and M.R. Syed, "Fast encryption for multimedia",IEEE Transactions on Consumer Electronics, vol. 47,101-107,Feb. 2001.

[Zaiane, et.al., 2002] Osmar R. Zaiane, Maria-Luiza Antonie, Alexandru Coman, "Mammography Classification by an Association Rule-based Classifier", MDM/KDD 2002: International Workshop on Multimedia Data Mining (with ACM SIGKDD 2002).

[Zhang, Rosin, 2003] X. Zhang and P.L. Rosin, 'Superellipse fitting to partial data', Pattern Recognition, vol. 36, no. 3, pp. 743-752, 2003

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.