Available Online at http://www.recentscientific.com

International Journal of Recent Scientific Research
Vol. 6, Issue, 8, pp.5731-5736, August, 2015

ISSN: 0976-3031

International Journal of Recent Scientific Research

RESEARCH ARTICLE

EFFECTIVENESS OF GAUSSIAN AND AVERAGE NOISE REDUCTION FILTERS ON IDEAI FINGERPRINT IMAGE IN BIOMETRIC FINGERPRINT IDENTIFICATION SYSTEM

1*Syed Mohsin Saif, 1Mudasir Manzoor Kirmani and 2Ziema Mushtaq

1Dept. of CS & IT, School of Computer Science and Information Technology, MANUU, Hyderabad
2Dept. of Computer Science, Kashmir University Srinagar, Hyderabad JK

ARTICLE INFO

Article History:

Received 5th, July, 2015
Received in revised form 12th, July, 2015
Accepted 6th, August, 2015
Published online 28th, August, 2015

Key words:

Biometrics, Fingerprint identification and verification, Noise, filters and histogram.

ABSTRACT

Privacy, prevention, protection and accessibility of the organizational data became the grave concern for all the organization of varying scope and service. Each data variable has to be protected from being accessed by malicious users. All the accesses to the system should be identified and verified before being granted permission to use the system. Many practices are in place to restrict the malicious users from making their entry into system. Biometric security systems have been gaining much more popularity. Fingerprint identification and verification system has faced many challenges to make the perfect matching efficient. In nature to get ideal condition is very rare. Biometric fingerprint systems do face similar challenges. Noise is most predominate factor which makes the system to withstand certain challenges. An attempt has been made in present study to find the behavior of noise and the counter measures to enhance to image more or less similar to the original image by applying some filters.

INTRODUCTION

Nature is dynamic, human beings being the most ardent creations on the earth have always been indulged both legally as well as illegally in the thrust of acquiring the information to squeeze more and more benefits by executing it to explore and acquire the gain and control over the resources for achieving self sufficiency and self reliance in both qualitative as well as quantitative parametric characteristics. The practice of acquiring information by peeing across the restricted zones of corporate information repositories leaves the parent system rather organization into danger of losing their coverage , turnover and other related characteristics of survival and serviceability.

To design the proactive procedures and strategies for designing, developing and implementing new systems, each organization leaves almost no stone unturned to frame the security infrastructure to make their all information secure so that no intruder can get any chance to access these sensitive information and vital data repositories of any organization.

Security has been always a challenging perspective to deal, so as to ensure the safety and other related characteristics of the system. It is the core agenda of concern for every small or large, public and private sector domains. From time to time there were different protocols to combat the issues which were conceived to be fatal for the organization's setup.

Once security is sought, identification and verification of the requisite person who intends to claim the accessibility to the system are the main milestones to be framed with firm, efficient, robust and reliable standards. Once these measures are worthy enough to stand, any kind of security breach can be dealt with great reliability.

Identification and verification are the most important and challenging aspects of any security establishment. There are number of such techniques available to support the security of such systems Among them some popular methods were traditional personal identification, knowledge based identification, token based identification/ smart card based identification etc. However, since these traditional approaches are not based on the inherent attributes of an individual to make a personal identification, they have a number of disadvantages like token may be lost, stolen, forgotten, or misplaced, PIN may be forgotten or guessed by the imposters. These Approaches are also unable to differentiate between an authorized person and the imposter who fraudulently acquires the token or knowledge of the authorized person [1, 2, 3, 4].

Corresponding author:* **Syed Mohsin Saif
Dept. of CS & IT, School of Computer Science and Information Technology, MANUU, Hyderabad

A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. To achieve this motive biometrics is believed to be the unique and universal approach for automatic individual identification[5].

Biometric System

Biometric technologies are becoming the foundation of the extensive array of highly secure identification and personal verification solutions. Physiological characteristics include fingerprint, face recognition, hand geometry, iris, palm, vascular pattern etc. Behavioral characteristics are the traits that are learned or acquired like dynamic signature verification, speaker verification, gait, key stroke dynamics etc. [6].

Biometrics has not only engulfed the premises of the closed structures but has quite dominantly overpowered open system such as enterprise-wide network security infrastructures, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, health and social services .Apart from this many countries have adopted the biometrics oriented security measures in passport, VISA, public ID programs as well [7].

A biometric system is essentially a pattern recognition system which make a personal identification by determining the authenticity of a specific physiological or behavioral characteristics possessed by the client. The block diagram of a generic biometric system is shown in figure 1 below, logically, it can be divided into three modules: Enrollment module, verification module and identification module, where as last two are the post enrollment module.

- ***Enrollment module:*** The enrollment module is responsible for enrolling individuals into the biometric system. During the enrollment phase, the biometric characteristics of an individual are first scanned by a biometric reader to produce a raw digital representation of the characteristics.
- ***Verification module:*** The verification is often referred to as 1:1(one-to-one) matching [8]. The verification module is responsible for verifying the individuals at the point of access. Nearly all verification systems can render a match/or no-match decision in less than a second. The system that requires the clients to authenticate their claimed identities before granting the access to the secure system is a verification application [8].
- ***Identification Module:*** The identification module works little different than the verification module in the sense that identification system does not require the person to identify. Identification checks the biometric against the stored reference templates in the database, if the biometric sample showed the positive matching percentage, there is a good probability the individual has been identified [9].

Apart from these main modules there are several other entities which are considered as the vital domain of any biometric personal identification system. The brief discussions of these are mentioned as under:

a. ***Reader/Scanner:*** A biometric sensor such as a fingerprint scanner is one of the central pieces of biometric capture module. This captured digital representation of biometric sample characteristics is known as sample.

b. ***Feature Extractor/Processor:*** To facilitate the biometric matching, the input sample obtained via scanner, the raw digital representation is processed by the feature extractor to generate a compact but expressive representation called a feature set.

c. ***Template Creation and Storage:*** A pattern of interest called a feature set is enrolled and saved into the template database. The feature set or template can be obtained from the input sample by rendering different algorithms as per the specification. This enrollment template is sometimes called as reference.

d. ***Matching/Comparing:*** The biometric reference template which has been already acquired from the individual and stored in database is matched with the newly enrolled reference of the individual on the bases of some minutiae pattern present on ones specific biometric trait.

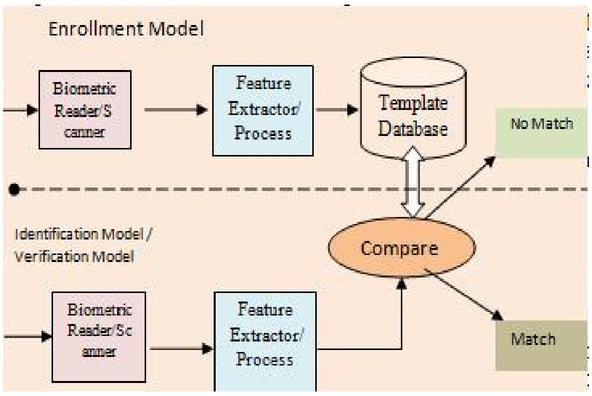

Enrollment Model
Biometric Reader/S canner
Feature Extractor/ Process
Template Database
No Match
Identification Model / Verification Model
Compare
Biometric Reader/Sc anner
Feature Extractor/ Process
Match

Figure 1 Generic Biometric fingerprint identification and verification system

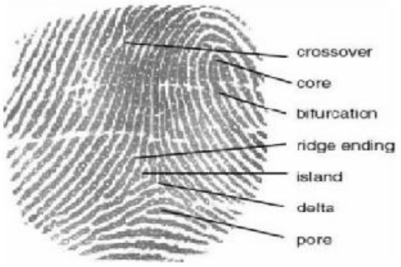
Fingerprints

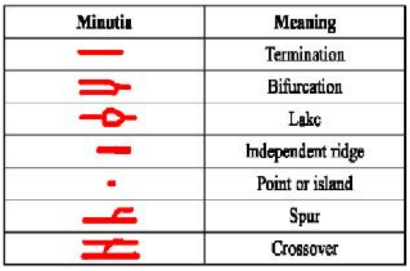
Fingerprint has been the most popular biometric trait used in designing a biometrics to setup mechanism for personal identification and verification. Fingerprint identification as well as verification systems have been deployed in a wide range of application domains and perspectives to ensure better and efficient security levels. Almost from small personal gadgets to big data repositories, every source nowadays have been secured form all criminal intruders like masqueraders, clandestine or misfeasors by introducing biometrics Fingerprints, the patterns of ridges and valleys on the “friction ridge” surfaces of fingers, have been used in forensic applications for over a century. Friction ridges are formed in uterus during fetal development, and even identical twins do not have the same fingerprints [10]. The recognition performance of currently available fingerprint-based recognition systems using prints from multiple fingers is quite good

Figure 2 fingerprint, pattern of ridges and furrows

The first latent fingerprint identification came in1880 by Dr. Henry Faulds He discussed fingerprints as a means of personal identification, and the use of printers ink as a method for obtaining such fingerprints. He is also credited with the first fingerprint identification of a greasy fingerprint left on an alcohol bottle.

To design the fingerprint identification system we need to have cameras/sensors or scanners to obtain the fingerprint of the individual. Than the obtained fingerprint is subjected to be processed to extract the reference template or template which will serve as the main token for identification and match to claim the identity. Fingerprint-based biometric systems use a combination of acquisition devices, background software and algorithms, and advanced database systems to complete tasks[11]. As with all biometric technology, the first step in implementing a fingerprint system is enrollment





Minutia	Meaning
	Termination
	Bifurcation
	Lake
	Independent ridge
	Point or island
	Spur
	Crossover

Finger print sensors

To obtain the digital pattern of the image we need to capture the real fingerprint pattern (ridges and valleys on the surface of the fingertip). We require a high quality sensor/scanner to facilitate versatility in capturing the images. Sensors like live sensing, frustrated total internal reflection (FTIR) method, direct optical imaging method are gaining popularity [12]. Apart from this optical fiber and light emitting polymers also exit which also support the sample scanning. These sensors are source from which the biometric fingerprints are captured and considered as input sample for biometric verification and identification system. These biometric traits are later stored in a centralized database for verification and matching process.

Noise

Presence of any unwanted signal which deforms the quality of the image (fingerprint) hence causes inaccuracy while interpreting the image. This unwanted signal may get into the image in various ways: either the quality of the original image to be enrolled is not worthy enough to get good minutiae extracted from the image or can be problem in the sensor while acquiring the image [13]. Some events which can introduce noise in the image are:

- Orientation and localization of the finger on the sensor.
- Displacement or partial overlap of the finger on the sensor area.
- Non-linear distortion or pressure and skin conditions.
- Sensor robustness and reliability.

Noise makes the fingerprint recognition system to be less accurate and less reliable. The false acceptance and false rejection ratio may show drastic inclination or declination in their behavior. Noise cannot only be the result of the physical condition of the finger or the behavior of the sensor environment; it can be introduced by the impairments in the medium when the fingerprint is transmitted from one source to another destination.

Types of Noise

There are different types of noises which can be resultant of the different situation in the sensor environment or trait enrollment condition. Few popular noise types which may cause either Additive, multiplicative or random noise effects on the image are simulated by using Mat-lab are:

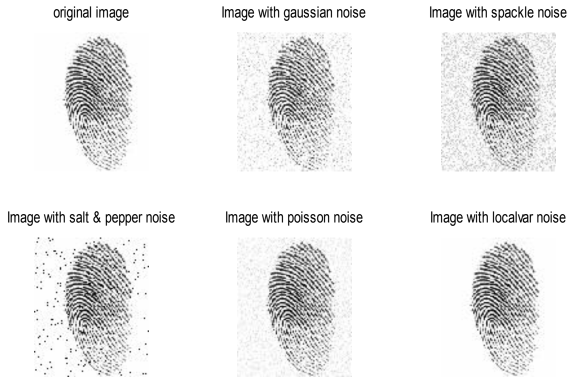

original image
Image with gaussian noise
Image with spackle noise
Image with salt & pepper noise
Image with poisson noise
Image with localvar noise

Figure 3 Same input images (original) with different simulated noise treatments

Gaussian Noise

The Gaussian Noise Generator block generates discrete-time white Gaussian noise. It is additive noise, caused by the random fluctuations in the signal. This type of noise can be observed while watching a television and channel gets slightly mistuned to different frequency.

The probability density function of *n*-dimensional Gaussian noise is

$$f(x) = ((2\pi)^n \delta K)^{-1/2}\, e^{\left((-x-u)^T K^{-1} \frac{(x-\mu)}{2}\right)}$$

Where x is a length-n vector, K is the n-by-n covariance matrix, μ is the mean value vector, and the superscript T indicates matrix transpose.

Figure 4 (I) original image with stimulated gaussian noise (Variance=0.07,Mean= 0.02)),(II) noised image

Speckle Noise

Speckle noise is a granular noise that inherently exists in and degrades the quality of image. It increases the mean grey level of a local area [14].Speckle noise is a high frequency component of the image and appears in wavelet coefficient [15]. Speckle noise affects all coherent imaging systems including medical ultrasound.

The acquired image is thus corrupted by a random granular pattern, called speckle that delays the interpretation of the image content. A speckled image is commonly modeled as $v_1 = f_1\vartheta$:

Where $f = \{f_1, f_2, f_3, ... f_n\}$ = is a noise-free ideal image,
$V = \{v_1, v_2, v_3 ......v_n\}$ speckle noise and
$\vartheta = \{\vartheta_1, \vartheta_2, \vartheta_3, ... \vartheta_n\}$ is a unit mean random field.

Original image when treated with simulated speckle noise with variance of 0.02, the quality of the image degraded as shown in Figure 5.3(II)

Figure 5 original image with stimulated speckle noise (Variance=0.02),(II) noised image

Random Noise

Random noise is characterized by intensity and color fluctuations above and below the actual image intensity. There will always be some random noise at any exposure length and it is most influenced by ISO speed. The pattern of random noise changes even if the exposure settings are identical [16]. The image M with random noise was generated by adding random noise of 0.01 variance and 0.5 mean randn() function in Matlab.

$$\mathrm{M} = \mathrm{I} + \vartheta \times (\mathrm{randn}(\mathrm{size}(\mathrm{I}) - \mathrm{m}$$

where M is the noised image obtained after adding randomized noise of variance ϑ and mean m on the original image I. randn(), generates arrays of random numbers with the size equal to the size of original image I.

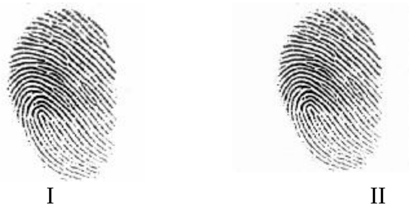


Figure 6 original image with stimulated random noise (Variance=2,Mean= 0.5)),(II) noised image

Image Enhancement

Image enhancement is the task of applying certain transformations to an input image such as to obtain a visually more pleasant, more detailed, or less noisy output image. Image enhancement techniques can be divided into two broad categories:

1. Spatial domain methods, which operate directly on pixels, and
2. Frequency domain methods, which operate on the Fourier transform of an image.

Noise Reduction Filtering

The purpose of smoothing is to reduce noise and improve the visual quality of the image. Often, smoothing is referred to as *filtering*. Image filtering is useful for many applications, including smoothing, sharpening, removing noise, and edge detection [17]. A filter is defined by a kernel, which is a small array applied to each pixel and its neighbors within an image. In most applications, the center of the kernel is aligned with the current pixel, and is a square with an odd number (3, 5, 7, etc.) of elements in each dimension. The process used to apply filters to an image is known as convolution, and may be applied in either the spatial or frequency domain.

Averaging Filtering

Mean filtering is a simple, intuitive and easy to implement method of *smoothing* images, *i.e.* reducing the amount of intensity variation between one pixel and the next. It is often used to reduce noise in images [18].

Suppose we have n number of images, each with noise, then i^{th} noisy image will be

$\mathrm{M} + \mathrm{N}_i$

Where M is the Matrix of original noise free image, N_i is a matrix of normally distributed random values with mean 0. We can find the mean M' of these images by simple add and divide method.

$$M' = \frac{1}{n}\sum_{i=1}^{n}(M + N_i) = \frac{1}{n}\sum_{i=1}^{n} M \frac{1}{n}\sum_{i=1}^{n} N \qquad N = N_1, N_2, N_3, ..., N_n$$

$$= M + \frac{1}{n}\sum_{i=1}^{n} N_i$$

Since, N_i is normally distributed with mean 0; it can be readily shown that the mean of all the N_i's will be close to zero, greater the number of N_i's, the closer to zero. Thus After applying the [3, 3] Averaging filter on the above noised images we obtained the enhanced images with less noise effects as shown in figure 6.3 below;

Gaussian noise	Speckle noise	Random noise

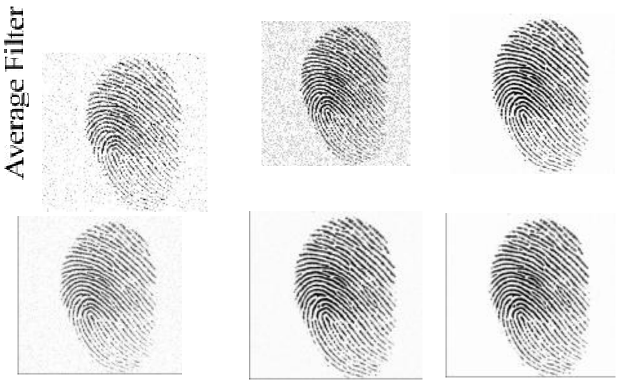


Figure 7 images obtained after [3x3] Average noise reduction filtering on the noised images

Gaussian Filter

The Gaussian smoothing operator is a 2-D convolution operator that is used to `blur' images and remove detail and noise. In this sense it is similar to the mean filter, but it uses a different kernel that represents the shape of a Gaussian (`bell-shaped') hump. This kernel has some special properties which are detailed below. The Gaussian distribution in 1-D has the form:

$$G(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{x^2}{2\sigma^2}}$$

Where σ is the standard deviation of the distribution.

Gaussian noise	Speckle noise	Random noise

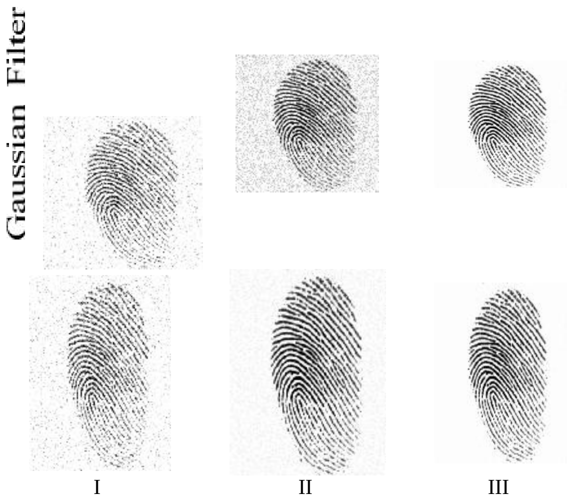
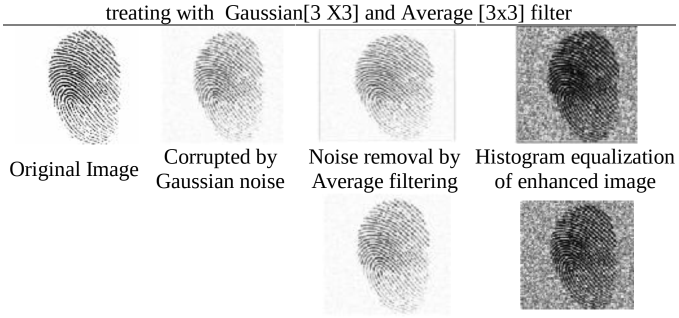


Figure 8 images obtained after [3x3] Gaussian noise reduction filtering on the noised images

Histogram And Histogram Equalization

A. Histogram Equalization of the image corrupted with Gaussian noise after treating with Gaussian[3 X3] and Average [3x3] filter



Original Image

Corrupted by Gaussian noise

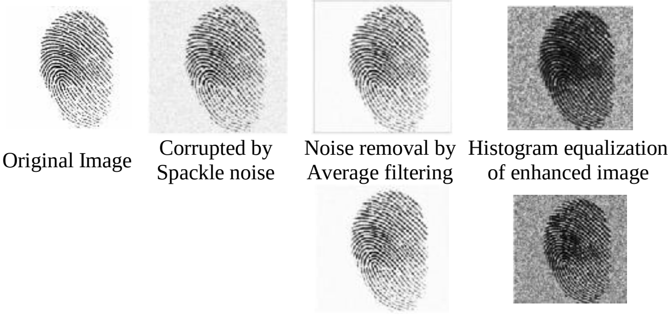
Noise removal by Average filtering

Histogram equalization of enhanced image

Noise removal by Gaussian filtering

Histogram equalization of enhanced image

B. Histogram Equalization of the image corrupted with Spackle Noise after treating with Gaussian[3 X3] and Average [3x3] filter



Original Image

Corrupted by Spackle noise

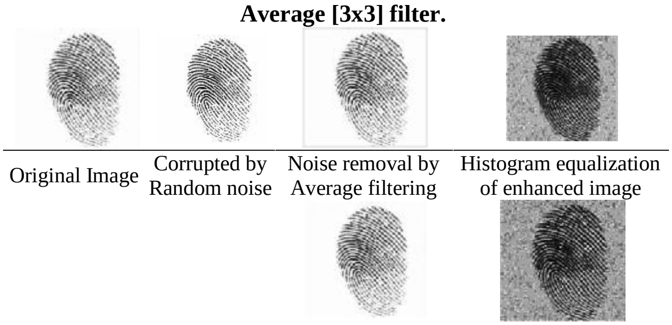
Noise removal by Average filtering

Histogram equalization of enhanced image

Noise removal by Gaussian Filtering

Histogram equalization of enhanced image

C. Histogram Equalization of the image corrupted with Random Noise after treating with Gaussian[3 X3] and Average [3x3] filter.



Original Image

Corrupted by Random noise

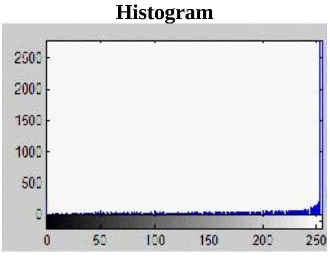
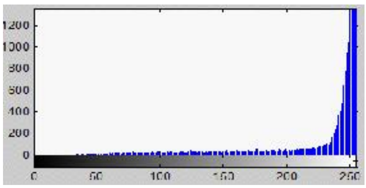
Noise removal by Average filtering

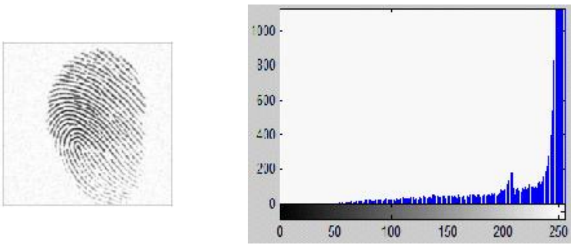
Histogram equalization of enhanced image

Noise removal by Gaussian Filtering

Histogram equalization of enhanced image

Histogram of various fingerprint images

Image	Histogram
 Noise free	
 Currupted by Gaussain noise	



Enhanced by Average Filtering

CONCLUSION

Biometric Fingerprint identification system is very popular technique to design versatile mechanism for obtain security infrastructure to prevent illegal and malicious users to introduce the valuable assists of any organization. Apart from his popular applicability Biometric fingerprint system has got its limitation when it comes to identify and then verify the sample with the one stored in the central database. The study was conducted to explore the impact of additive, multiplicative and random noise on input image and then the enhancement of the corrupted images with various filters. The study showed that Gaussian and average filters have better performance in removing the noise and contribute to great extent for perfect fingerprint matching procedure.

References

Biometrics History, 2006, National Science and Technology council(NSTC) , Committee on technology, Committee on Home land and national security, Subcommittee on Biometrics., www.biometrics.gov.

Bockenbach, O. 2011. Fourier transform From Wikipedia, the free encyclopedia. [Online]. http://en.wikipedia.org/wiki/Fourier_transform.

Brandt, T. Classification Methods for Remotely Sensed Data, 2nd Edition. CRC Press.

Bremond, F. et al. 2006. Video-understanding framework for automatic behavior recognition, Behavior Research Methods, Vol. 30(3), 416-426.

Clarke, R. 1994. Human Identification systems: Management challenges and public policy issues, Information technology & People, vol.7(4), 6-37.

Claude, B. 2010. Biometrics & Security: Combining Fingerprints, Smart Cards and Cryptography, PhD thesis.

Clayton, M. 2010.US plans massive data sweep", Christian Science Monitor. Retrieved 10 January 2010.

Davies, S. 1994. Touching big brother: How Biometric technology will fuse flesh and machine", Information Technology & People, vol.7 (4), 60-69.

Fingerprint Recognition, BioEnable Technologies Pvt. Ltd., E-204, 3rd floor, Railway Station Complex, CBD Belapur, Navi Mumbai, MH, India, 2005.

Jagtap, V. 2010. Fast Fourier Transform Using Parallel Processing for Medical Applications, M Sc Thesis, Biomedical Engineering, University of Akron, Ohio.

Keith, A.R. 2003. "Information Security: Challenges in Using Biometrics" [Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census", Committee on Government Reform, House of Representatives (GAO-03-1137T)], United States General Accounting Office (GAO), 441 G Street NW, Room 7149, Washington, DC 20548.

Michael, P. 2004. Biometrics: An Overview of the Technology, Challenges and Control Considerations, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, vol.4.

Miller, B. 1994. Vital signs of identity .IEEE, Spectrum, vol.31 (2), 22-30..

Newham, E. 1995. The Biometric Report, SJB Services, New York.

Ruttenbur, W. 2006. Biometrics, Industry overview for the investment community", Morgan keegan & Company, Inc. Equity Research.

Salil, P. 2011. Biometric Recognition: sensor characteristics and image Quality, IEEE Instrumentation & Measurement Magazine.

Sudha, S. 2009. Speckle Noise Reduction in Ultrasound Images by Wavelet Thresholding based on Weighted Variance, *International Journal of Computer Theory and Engineering*, Vol. 1(1).

How to cite this article:

Syed Mohsin Saif *et al.*, Effectiveness Of Gaussian And Average Noise Reduction Filters On Ideal Fingerprint Image In Biometric Fingerprint Identification System. *International Journal of Recent Scientific Research Vol. 6, Issue, 8, pp.5731-5736, August, 2015*

****