Applied Mathematics & Information Sciences
*An International Journal*

http://dx.doi.org/10.12785/amis/081L04

# Chaos based Secure Storage and Transmission of Digital Medical Images

*Fahad bin Muhaya*[1,2], *Muhammad Usama*[1,*] *and Fahim Akhter*[1,2]

[1] Prince Muqrin Chair for IT Security (PMC), King Saud University, Riyadh, Saudi Arabia
[2] Management Information Systems Department, College of Business Administration, King Saud University, Riyadh, Saudi Arabia

Received: 10 Apr. 2013, Revised: 5 Aug. 2013, Accepted: 6 Aug. 2013
Published online: 1 Apr. 2014

**Abstract:** With the rapid and progressive development of medical images and data exchange in digital formats, information security and image encryption are becoming more important in data storage and transmission. Because of the widespread use of medical images in hospitals and healthcare communities, it is important to protect them from unauthorized access. In this paper, we propose a medical image encryption algorithm based on a chaotic technique. A chaotic logistic map is used to scramble the pixel values of a medical image. In order to achieve a high level of security, a simplified version of the Data Encryption Standard (DES) is used. In order to verify the higher level of security and performance with the proposed algorithm, an experiment analysis has been performed.

**Keywords:** Information Security, Digital Medical Images, Cryptography, Chaos based Encryption

## 1 Introduction

Information security and cryptography have always been important areas of research. Secure information sharing and communication is an essential part of many fields. In the growing fields of the internet and data communication technologies, there has been an increase in data sharing and the exchange of multimedia data. Secure data communication between users and/or organizations is becoming a critical and sensitive issue. Similarly, the security of multimedia images is an important part of many disciplines related to the medical sciences and technologies, e.g., telemedicine and healthcare centers. The storage and transmission of medical image data is a daily routine in these domains. The fundamental properties of a chaotic system have attracted the attention of many researchers and centers, including its ergodicity, sensitivity to initial conditions, system parameters, mixing properties, etc. These properties are very important and are needed in cryptography to obtain high quality encryption results. Chaotic systems are defined using pseudorandom sequences and created by nonlinear dynamics systems.

## 2 Proposed Algorithm

The proposed algorithm consists of two components: medical image scrambling and medical image encryption. Medical image scrambling is based on a chaotic technique, while medical image encryption is done using DES. A block diagram of the DES encryption and decryption computation process is shown in Figure 1. Image scrambling is an important part of the algorithm and is used to achieve a higher level of confusion. To design an unpredictable and secure implementation of the proposed algorithm, a differential equation based chaotic map has been utilized. To achieve a higher level of unpredictability and randomness in the scrambling process, the parameters of this differential equation have been chosen critically. The implementation of the proposed algorithm is flexible and each component is changeable. A chaotic map that provides good quality scrambling results can be replaced with the proposed chaotic map. In the proposed algorithm, a medical image is processed using a chaotic cat map to scramble the output images and achieve a higher level of confusion, after which the DES algorithm is used to perform encryption or decryption operations on the medical image. The combination of chaotic and block ciphers is more secure and complex compared to other algorithms

[*] Corresponding author e-mail: usama.khanzada@hotmail.com

and provides more features, as explained in [1]. Descriptions of each component are given in the next sub-sections.

## 3 Scrambling

In this paper, the concept of using a separate component for medical image scrambling is proposed to achieve a higher level of security and efficiency. In this process, the arrangement of the pixel values is changed from its original configuration to provide a higher level of confusion in the scrambling process. Other image scrambling and transformation techniques include a Baker map [2], affine transformation [3], knight-tour transformation [4], magic-square transformation [5], etc. Arnold's cat map and chaotic Baker map-based scrambling are more popular and applicable in research because of their high quality results. An encryption technique based on a chaotic Baker map was first introduced by Franz Pichler and Josef Scharinger. A chaotic Baker map is a two dimensional map that was further studied and extended into a three dimensional chaotic map in [6], which was then used to shuffle the pixel values of an image. In this paper, medical image scrambling is performed using a chaotic cat map.

### *3.1 Scrambling by Arnold's cat map*

Arnold first introduced two dimensional invertible chaotic maps in the 1960s. The generated pictorial output looked like the image of a cat, which earned it the name Arnold's cat map [7,8]. In matrix form, Arnold's cat map is described as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod(M) \qquad (1)$$

where $c$ and $d$ are constants, $n = 0, 1, 2, 3, .......$ ,$(x_n, y_n)$ is the location of a pixel value in a medical image.

$(x_{n+1}, y_{n+1})$ is the new location for the pixel value after performing transformation on the image, and$N$ is the number of iterations required for this transformation. Different numbers of iterations can produce different shuffling results. To provide the chaotic properties in the system, Arnold's cat map introduces tension by performing matrix multiplication and folding by a mod operation of the matrix, as shown in the equation. Arnold's cat map is effective at shuffling image pixel values. Changing the parameter values and image size removes the periodicity in Arnold's cat map, and the parameter values can be used as secret keys in the shuffling process. However, its periodicity is the weakness of Arnold's cat map because an image can be reproducible after performing several iterations, and the statistically shuffled and original images have the same values [9,10,11]. Arnold's cat map has been used to shuffle the pixel value position without modifying the pixel values [12]. Thus, the DES is used to achieve diffusion in the encryption process.

**Table 1** Initial Permutation $IP$ [13]

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

## 4 Data Encryption Standard (DES)

The most widely used symmetric block cipher is based on the DES adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Simple-DES and Triple-DES algorithms were designed in such a way that they may be used in many applications to protect data. The method of implementation will depend on the application and environment. The DES was designed to encrypt and decrypt blocks of data consisting of 8 bytes (64 bits) under the control of keys with the same size. Decryption requires the use of the same key as encryption. A 64-bit block passes through initial permutation $IP$, then to a complex key dependent computation, and finally to a permutation that is the inverse of the initial permutation $IP^{-1}$. A description of the computation of cipher function $f$ and key schedule is give below for the encryption and decryption. Finally, a definition for cipher function $f$ is given in terms of primitive functions, which are called the selection functions $Si$ and permutation function $P$.

### *4.1 Encryption*

First, the 64 bits of the input block are encrypted through initial permutation $IP$.

The permuted input block is then input to the complex key dependent computation described below. The output of that computation, called the preoutput, is then passed through a permutation that is the inverse of the initial permutation $IP^{-1}$.The computation, which uses the permuted input block as its input to produce the pre-output block, consists, except for a final interchange of blocks, of 16 iterations of a calculation that is described below in terms of cipher function $f$, which operates on two blocks, one of 32 bits and one of 48 bits, and produces a block of 32 bits. If we let a 64-bit input

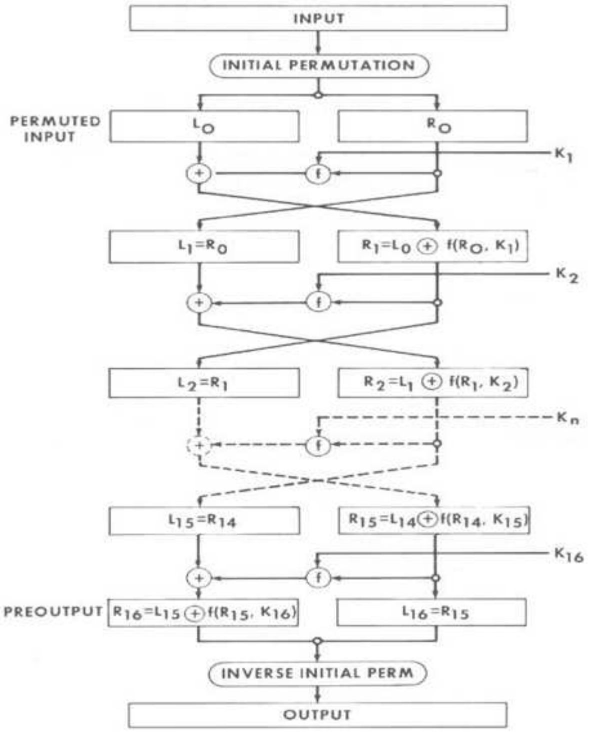


**Fig. 1** Encryption computation [13]

**Table 2** Inverse Initial Permutation $IP^{-1}$ [13]

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

Calculation of f(R,K)]

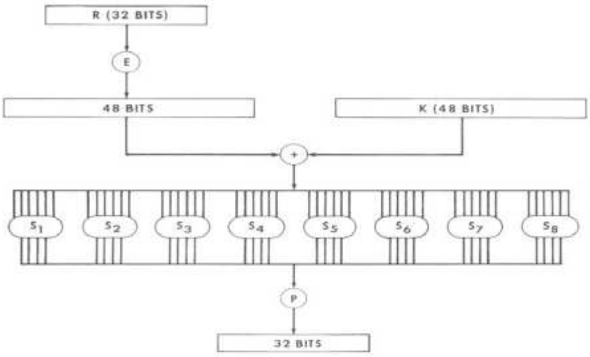


**Fig. 2** Calculation of f(R,K) [13]

block consist of two 32-bit blocks,$L$ and $R$ then this input block is represented as $LR$. A 48-bit block,$K_n$ is chosen from the 64-bit key; this selection, or key schedule [13], depends on the iteration number n.

$$K_n = KS(n, KEY)$$

Here,$KS$ is the key schedule function, n is the number of iterations from 1 to 16, and the 64-bit block,$KEY$ is input and gives a 48-bit block $K_n$ as an output. The 48-bit key $K_n$ and 64-bit permuted input block $L_nR_n$ are related as: [13]

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$

Here, the symbol $\oplus$ denotes a bit-by-bit "exclusive OR" or "XOR." The output of the 16th iteration $L_{16}R_{16}$ is then interchanged to produce pre-output block $R_{16}L_{16}$.

## 4.2 Decryption

The inverse permutation $IP^{-1}$ is applied to the pre-output block. To decrypt the encrypted block, the same algorithm is used, as expressed in the equation, and key $K$ is used to encrypt the block [13].

$$R_{n-1} = L_n$$
$$L_{n-1} = R_n \oplus f(L_n, K_n)$$

To decrypt permuted input block $R_{16}L_{16}$,$K_{16}$ is used during the 1st iteration, then $K_{15}$ for the 2nd, and so on until at the 16th iteration $K_1$ is used and $R_0L_0$ is the pre-output block of this process.

## 4.3 Cipher Function $F$

Let function $E$ take a 32-bit input block and provide a 48-bit output block by applying selection on the input bits as defined in Expansion Permutation $E$. Here, we have eight standard unique selection functions or S-boxes:
$S_1, S_2, ........., S_8$

Each one takes a 6-bit input block and produces a 4-bit output. For example, selection function $S$ selects six sequential bits $6j-5, 6j-4, ...., 6j$ from the 48-bit input block. Similarly, it selects six sequential bits $4j-4, 4j-3, ...., 4j+1(mod 32)$ from the 48-bit key $K$. The two consecutive selection functions share two bits with each other, e.g., selection function $S_1$ uses $32, 1, 2, 3, 4, 5$ bits and second selection function $S_2$ uses

**Table 3** Expansion Permutation (E) [13]

| | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

**Table 4** Permutation Function (P) [13]

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

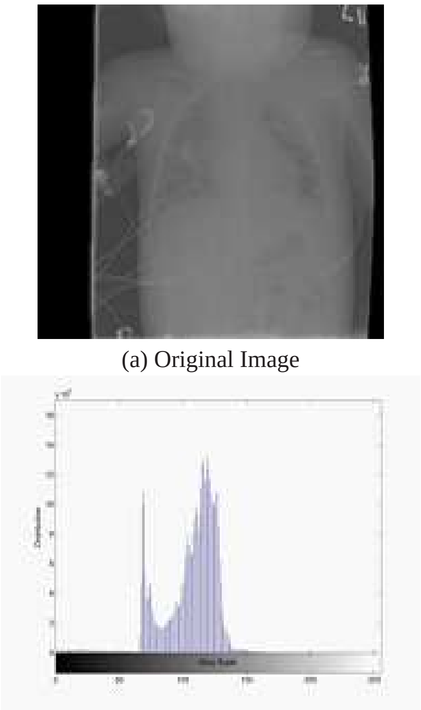
$4, 5, 6, 7, 8, 9$ bits, with bits $4$ and $5$ shared. Note that this bit sharing does not apply to the key bits on one round. The 32-bit output block of the eight selection functions is then permuted using permutation function $P$ to obtain a 32-bit output block. This 32-bit permuted block is the output of function $f(R, K)$ for inputs $R$ and $K$.

## 5 Experiment Results

An ordinary computed radiography (CR) image, as shown in Figure 3(a), having a size of 5,121,974 bytes and a resolution of 2500 × 2048, is used for the experiments and analysis. The image has been enhanced using a contrast optimization process. Therefore, it should not require any further processing in any display environment. The encrypted and decrypted images are given in Figures 4(a) and 5(a), respectively, to prove the robustness and quality of the encryption results. The encrypted medical image is totally scrambled and highly secure from unauthorized access and illegal use. The decrypted medical image is the same as the original image, with no changes and/or alterations. Thus, the proposed enhancements are reversible and reliable for storage and transmission.

### *5.1 Histogram Analysis*

We selected several test medical images of different sizes and different contents and calculated their histograms. A typical experiment result from these are given in Figures 3,4 and 5. In Figure 3(b), a histogram of the original medical image is given, while Figure 4(b) presents a histogram of the encrypted medical image. The experiment results show that the histogram of the encrypted medical image is fairly uniform and different from the original medical image.



(a) Original Image

(b) Histogram of Original Image

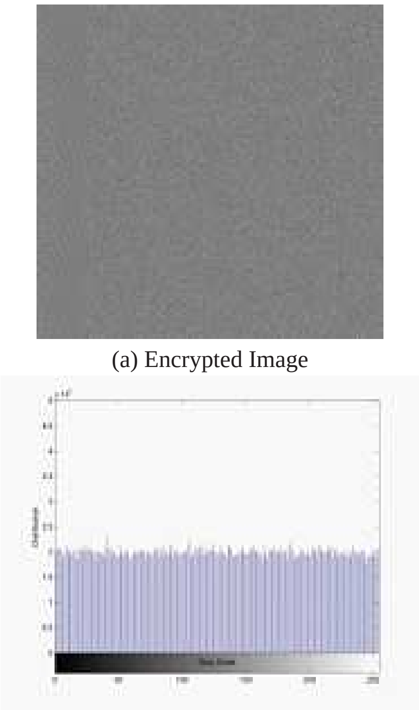
**Fig. 3** Histograms of Original Image

### *5.2 Correlation Coefficient Analysis*

The achievable confusion and diffusion results are given by performing experiments on the correlations of adjacent pixels in the encrypted medical images [14]. To perform correlation analyses between two vertically adjacent pixel values, two horizontally adjacent pixels, and two diagonally adjacent pixels in the encrypted medical image, the following process was carried out. The correlation coefficient analyses performed using the given formula:

$$\begin{aligned} r =& \frac{cov(x,y)}{\sigma_x \sigma_y} \\ =& \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \end{aligned} \tag{2}$$

Where $r$ is correlation coefficient. In Table 5, we give the correlation coefficients for the original, encrypted and decrypted medical images are shown in Figures 3, 4 and 5. It is clear from computed experimental results of these figures that there is negligible correlation between the these images.



(a) Encrypted Image

(b) Histogram of Encrypted Image

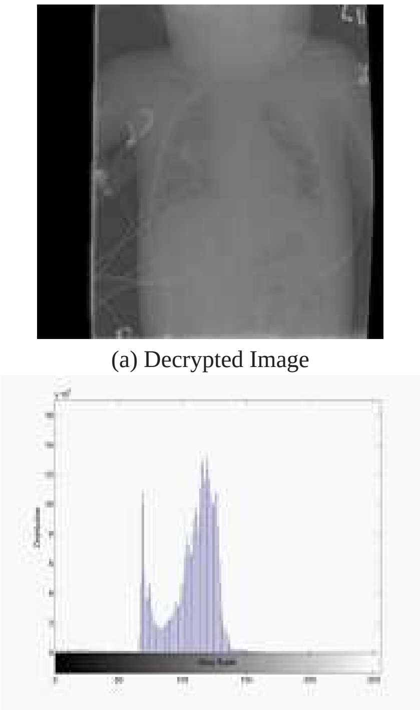
**Fig. 4** Histograms of Encrypted Image

**Table 5** Correlation coefficients of experimental results

| Medical Image | Test Image A | Test Image B | Test Image C |
|---|---|---|---|
| Mode | CBC | ECB | CFC |
| $r$ for Encryption | 0.003 | 0.0011 | 0.0012 |
| $r$ for Decryption | 1 | 1 | 1 |

### *5.3 Performance Analysis*

Apart from the importance of the quality and security, some other issues with medical image encryption operations are also vital. These include the efficiency and performance for real-time application. The algorithm for the proposed medical image encryption technique is implemented using the Microsoft visual C sharp programming language. The performance analysis was done on a 2.4 GHz Pentium IV with 2 GB RAM running the Windows 7 operating system. To achieve accurate experiment results for the performance, each test was executed 5 times, with the average times for the experiment results given in Table 6.



(a) Decrypted Image

(b) Histogram of Decrypted Image

**Fig. 5** Histograms Decrypted Image

## 6 Conclusion

Medical images have great importance because of the criticality of patient information and clinical treatment purposes. The unlawful, unauthorized, and illegal use or access of these images increases the importance of a security system. In this paper, a secure and efficient medical image encryption algorithm based on a chaotic map for medical image scrambling and DES for image encryption and decryption has been proposed to achieve a higher level of efficiency and security in medical image storage and transmission. A higher level of quality and performance was proven through experiment analyses on different sample medical images. The results have been

**Table 6** Performance Analysis

| Medical Image | Test Image A | Test Image B | Test Image C |
|---|---|---|---|
| Image Size in bytes | 5,121,974 | 1,782,140 | 1,413,518 |
| Dimension | 2500 × 2048 | 1200 × 1467 | 721 × 1760 |
| Encryption Time (sec) | 2.0625 | 0.140625 | 0.453125 |
| Decryption Time (sec) | 2.03125 | 0.171875 | 0.4375 |

analysed thoroughly to study the strength of the confusion and diffusion properties, security and resistance level against some known attacks. Experiment results indicate that the pixel value distribution in the encrypted images is even and uniform. Thus, the proposed algorithm is suitable and practical for real-time applications, in order to keep the storage and transmission processes for critical and confidential medical images secure and reliable.

## References

[1] M. Caglar, A Long-Range Dependent Workload Model for Packet Data Traffic. Mathematics of Operations Research, **29**, 92-105 (2004).

[2] A. Chydzinski, Time to Reach Buffer Capacity in a BMAP Queue, Stochastic Models, **23**, 195-209 (2007) .

[3] E. Cinlar, Introduction to Stochastic Processes, Prentice Hall Press, (1975) .

[4] E. Cinlar, Probability and Stochastics, Springer, (2011)

[5] D. R. Cox, P. A. W. Lewis The Statistical Analysis of Series of Events, Methuen, London, (1966).

[6] B. D'Auria, G. Samorodnitsky, Limit Behavior of Fluid Queues and Networks, Operations Research, **53**, 933-945 (2006).

[7] G. Fay, F. Roueff, P. Soulier, Estimation of the Memory Parameter of the Infinite-Source Poisson Process, Bernoulli, **13**, 473-491 (2007).

[8] D. Gross, C. M. Harris Fundamentals of Queueing Theory, John Wiley, (1998).

[9] J. M. Harrison, A.J. Lemoine A Note on Networks of Infinite-Server Queues. J. Appl. Prob., **18**, 561-567 (1981).

[10] D. Heath, S. Resnick, G. Samorodnitsky, Heavy Tails and Long Range Dependence in On/Off Processes and Associated Fluid Models, Mathematics of Operations Research, **23**, 145-165 (1998).

[11] M. Iftikhar, T. Singh, B. Landfelt, M. Caglar, Multiclass G/M/1 Queueing System with Self-Similar Input and Non-preemptive Priority. Computer Communications, **31**, 1012-1027 (2008).

[12] M. Iftikhar, B. Landfelt, M. Caglar, Towards the Formation of Comprehensive SLAs between Heterogeneous Wireless DiffServ Domains, Telecommunication Systems, **42**, 179-199 (2009).

[13] I. Kaj and M. S. Taqqu, Convergence to Fractional Brownian Motion and to the Telecom Process: the Integral Representation Approach. In Brazilian Probability School, 10th Anniversary Volume, Eds. M. E. Vares, V. Sidora Vicius, (2007).

[14] A. F. Karr, Point Processes and their Statistical Inference, Marcel Dekker, (1991).

[15] T. Konstantopoulos and S. Lin, Macroscopic Models for Long-Range Dependent Network Traffic. Queueing Systems, **28**, 215-243 (1998).

[16] W. E. Leland, M. S. Taqqu, W. Willinger, D.V. Wilson, On the Self-Similar Nature of Ethernet Traffic (Extended version), IEEE/ACM Transactions on Networking, **2**, 1-15 (1994).

[17] K. Maulik, S. Resnick Small and Large Time Scale Analysis of a Network Traffic Model. Queueing Systems, **43**, 221-250 (2003).

[18] T. Mikosch, S. Resnick, H. Rootzén and A. Stegeman Is Network Traffic Approximated by Stable Lévy Motion or Fractional Brownian Motion? Annals of Applied Probability, **12**, 23-68 (2002).

[19] I. Norros, A Storage Model with Self-Similar Input. Queueing Systems, **16**, 387-396 (1994).

[20] R. D. Reiss, Approximate Distributions of Order Statistics, Springer-Verlag, (1989).

[21] S. Ross, Introduction to Probability Models, Academic Press, (2007).

[22] H. P. Schwefel, L. Lipsky, Impact of Aggregated Self-Similar ON/OFF Traffic on Delay in Stationary Queueing Models (extended version). Performance Evaluation, **43**, 203-221 (2001).

[23] G. Samorodnitsky and M. S. Taqqu, Stable Non-Gaussian Random Processes, Chapman & Hall, (1994).

**Fahad bin Muhaya** is the Director of Prince Muqrin Chair (PMC) for IT Security and Dean of College Applied studies and community service at King Saud University. He holds a Ph.D., Masters and Bachalors degrees in Information Systems from George Maison University USA, Boston University USA and King Saud University respectively. He has worked and done research at numerous institutions in the Saudi Arabia. He is a member in number of scientific local and international associations, board member and founder of number of associations. He published number of scientific researches in trusted local and international magazines, he is an arbitrator for a number of conferences; he organized workshops in Saudi Arabia, and in some of global States in cooperation with international associations. He runs number of important activities in society service to spread education in information security.

**Muhammad Usama** is the Lecturer in the Prince Muqrin Chair (PMC) for IT Security at King Saud University, Saudi Arabia. He holds a Masters and Bachelors degrees in Software Engineering from Bahria University, Karachi, Pakistan. He has worked and done research at numerous institutions in the Pakistan and Saudi Arabia. His research focuses on the information security and cryptography. He has published research in conferences and journals.

**Fahim Akhter** is an Associate Professor in the Department of Management Information Systems, College of Business Administration at King Saud University, Saudi Arabia. He holds a Ph.D. in Computing Informatics, Master in International Business and a Bachelors degree in Management Information Systems form University of Bradford, Lindenwood University and University of Missouri St. Louis respectively. He has 20+ years of experience in research, teaching and services at Colgate University, Baruch College, Zayed University and King Saud University. He has worked and done research at numerous foreign institutions in the USA, United Arab Emirates, and Saudi Arabia. His research focuses on the expert system that would assist consumers to perform safe online decision-making transactions. He has published research in conferences and journals and served on the editorial boards of journals. He is the founding member of International Symposium on Web Services at Zayed University in 2008, 2009, 2010 and 2011. He has been invited to speak at universities and symposiums on a national and international level.