Advanced Image Encryption and Decryption Using Sandwich Phase Diffuser and False Image along with Cryptographical Enhancement

Abraham Panicker.O[a], A.Jabeena[a], Abdul Hassan Mujeeb[b]

[a] Photonics and Microwave Division, School of Electronics Engineering (SENSE), VIT University, Vellore, Tamilnadu - 632 014, India
[b] International School of Photonics, Cochin University of Science and Technology, Cochin-22, Kerala, India

***Abstract*- The revolution in communication technology facilitates fast and reliable information transfers and is being increasingly used in various fields like scientific, military, civilian and economic. Apart from the speed and reliability, security in transferring the information is gaining much importance now days. Optical data transfer offers several dimensions in which information can be hidden such as phase, polarization, and wavelength, etc., making it possible to encode data more securely. In addition to this, the characteristics of fast computing and the inherent parallelism of optical data transfer make it very useful for real-time applications. This paper focuses on the encryption and decryption of two-dimensional images. The encryption is done by employing a sandwich phase diffuser made by using two speckle patterns, and placed in the Fourier plane of a double random phase encoding system. After phase diffusion another image is fused to the resultant image and then cryptographical enhancement is done which provide an additional security to the system. The used cryptographic technique is derived from the AES cryptosystem in which a modified shift row operation is performed. During decryption first inverse cryptographical enhancement is done, followed by subtraction of fused image. Then further decryption process will be done. Reliability of the technique is evaluated using Mean Square Error (MSE) calculation between the decrypted and original image. In addition to MSE estimation, histogram and correlation coefficient analysis is performed.**

Keywords: Optical image encryption/decryption, Sandwich phase diffuser, laser speckle pattern, cryptographical enhancement, false image fusion.

I. INTRODUCTION

The revolution in information transfer technology facilitates fast and reliable information transfers and is being increasingly used in various fields like scientific, military, civilian and economic. Apart from the speed and reliability, security in transferring the information is having high importance, and this has motivated researchers to make the data security and transfer systems more secure. A. Kumar and K. Singh, in 1994, investigated the properties of elongated speckle patterns in the context of effect of aberrations on the speckle shape [1]. In 1995, N. Towghi, B. Javidi and Z. LuoJ shown that a fully phase-based encryption performs better than the amplitude-based encryption in the presence of additive noise, with respect to the Mean Square Error (MSE) [2]. Later, in 2000, X. Tan, O. Matoba, T. Shimura, K. Kuroda, B. Javidi an enhanced method for security of the data was developed where amplitude information of the object was replaced with the phase encoded information at the input plane which was done by modifying existing double random phase encoding architecture [3]. A new way of image encryption scheme was proposed by N.K. Pareek, Vinod Patidar, K.K. Sud, in 2006, which uses two chaotic logistic maps and an external key of 80-bit. The initial conditions needed for logistic maps where derived from an external secret key. Eight different operations where used to encrypt the pixels of an image and selection of operation used for a particular pixel depends on the outcome of the logistic map.

After encrypting a block of sixteen pixels of the image, the secret key will be modified for more security. Reliability of algorithm was analyzed using statistical analysis, sensitivity analysis, key space analysis etc. [4]. A highly secure encryption and decryption system using a sandwich diffuser made with two normal speckle patterns in the Fourier plane has been investigated [5]. Weimin Jin, Caijie Yan proposed an encryption algorithm which uses multichannel fractional Fourier transform (FRT) and double random phase encoding technique which encrypt images through different channels [6]. Michele De Santis and Giuseppe Schirripa Spagnolo proposed an asymmetric cryptography, as a part of holographic watermarking, which is able to detect malicious tampering. A fragile watermark is used which will be destroyed when someone tries to modify host image. But the proposed method was not suitable for the authentication of images transferred by Internet [7]. Encryption and decryption of a two-dimensional image using a sandwich phase diffuser was investigated by Madan Singh, Arvind Kumar, Kehar Singh, in 2008. Sandwich phase diffuser used is a combination of two elongated speckle patterns and it is placed in Fourier plane. Compared to the sandwich phase diffuser made using normal random phase diffuser, sandwich phase diffuser made using elongated speckle patterns makes the system less complicated [8]. Madan Singh, Arvind Kumar, Kehar Singh, in 2009, proposed an algorithm which uses a double random phase encoding system for encryption which utilizes 4f geometry. Input image is first modified by adding or multiplying other matrices before applying encoding to it [9]. Narendra Singh, Aloka Sinha, in 2009, proposed an algorithm which uses

978-1-4244-7286-4/10/$26.00 ©2010 IEEE

gyrator transform and chaos functions for image encryption [10].

This paper focuses on the encryption and decryption of two-dimensional images. The encryption is done by using a sandwich phase diffuser made by using two speckle patterns, and a false image which is added along with processed image at the final stage and this image is placed in the Fourier plane.

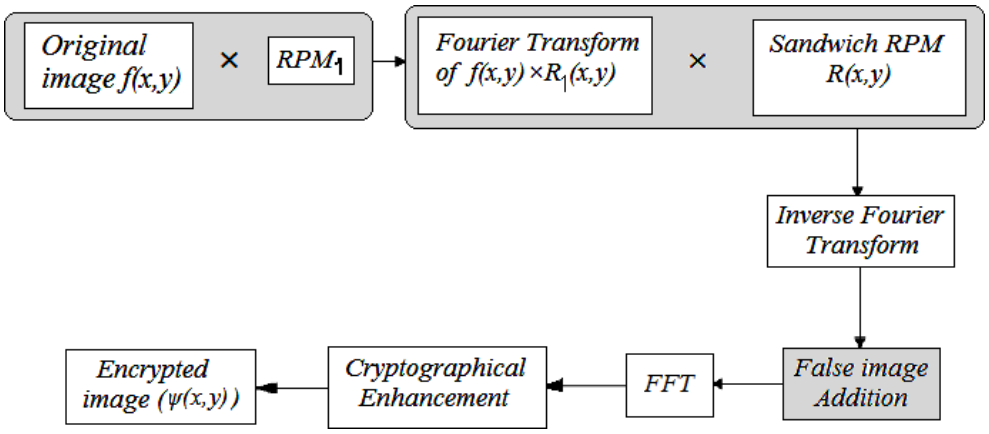

Fig. 1. Encryption Process

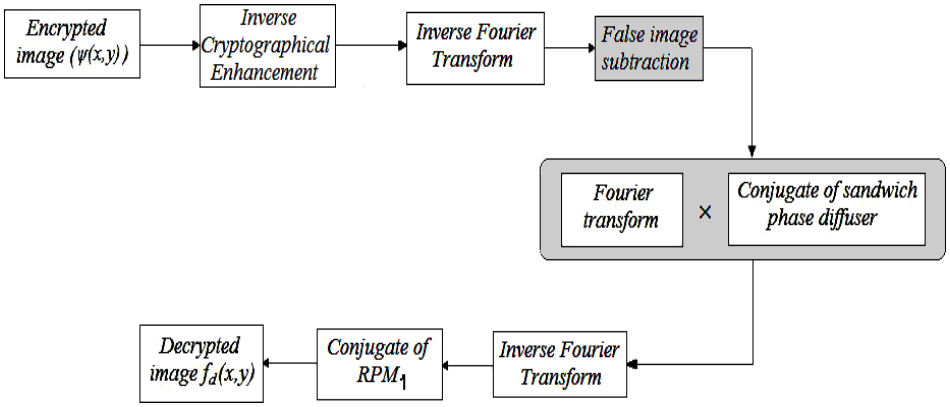

Fig. 2. Decryption Process

II. THEORETICAL ANALYSIS

Fig.1 shows the encryption of two-dimensional images is done by using in the Fourier plane of a double random phase encoding system, a sandwich phase diffuser made with two speckle patterns. Consider (x,y) denote the coordinates in the object Plane and (u,v) respectively and the Fourier transform. The real-valued function f(x,y) denotes the primary two-dimensional image to be encrypted, and function ψ(x,y) denotes the encrypted image. The encryption of the input image *f(x,y)* is done in two steps. First, the image *f(x,y)* is changed into a phase function and multiplied by the first random phase mask RPM1 denoted as $M_1(x,y)$ at the input plane. This product is then convolved with a sandwich random phase mask *M(x,y)* kept at the Fourier plane. Mask *M(x,y)* is made by using laser speckles and is the impulse response of the combination of the random phase masks RPM2 and RPM3 denoted as $M_2(u,v)$ and $M_3(u,v)$ respectively. The Fourier transform of the modified input image, i.e. the product of *f(x,y)* and $M_1(x,y)$, is passed through the combination of random phase masks $M_2(u,v)$ and $M_3(u,v)$ in the Fourier plane. The random phase functions $M_1(x,y)$, $M_2(u,v)$ and $M_3(u,v)$ are chosen to be statistically independent. The image encrypted by these random phase functions is given by:

$$\Psi_1(x,y) = \mathbf{IFT}\{\mathbf{FT}[f(x,y) \times M_1(x,y)] \times [M_2(u,v) \times M_3(u,v)]\}$$

$$\psi(x,y) = \mathbf{FT}\{\Psi_1(x,y) + F(x,y)\}$$

where $F(x,y)$ denotes false image, which is added at the final stage, **FT** denotes the Fourier transform operation and $\psi(x,y)$ denotes the encrypted image. $M_2(x,y)$ and $M_3(x,y)$ denote the inverse Fourier transforms of $M_2(u,v)$ and $M_3(u,v)$ respectively they are the impulse responses of the phase-only transfer functions $M_2(u,v)$ and $M_3(u,v)$, and thus provide stationary white noise. For decryption, shown in Fig.2, the Inverse Fourier transform of encrypted image is taken first and then the false image, which was added in the final stage of encryption process, is subtracted. Fourier transform of resultant image is taken and then it is multiplied with the conjugate of the combination of the random phase masks RPM2 and RPM3 denoted as $M_2(u,v)$ and $M_3(u,v)$. This product is then inverse Fourier transformed and multiplied with the conjugate of RPM1, $M_1(x,y)$, thus giving the decrypted image. The decrypted image may be expressed as

$$f_2(x,y) = \mathbf{IFT}[\psi(x,y)] - F(x,y)$$

$$f_1(x,y) = \mathbf{IFT}\{\mathbf{FT}[f_1(x,y)] \times Conj\{M_2(u,v) \times M_3(u,v)\}\}$$

$$f_d(x,y) = f_1(x,y) \times Conj\{M_1(x,y)\}$$

where $\psi(x,y)$ denotes the encrypted image, $F(x,y)$ denotes false image, and $f_d(x,y)$ denotes the final decrypted image.

III. SIMULATION RESULTS

The simulation study of proposed encryption/decryption algorithm was carried out in MATLAB 7.5 platform. A 256×256 pixels gray-scale image was used for study which was later replaced with an N×N pixels gray-scale image. The input image $f(x,y)$, shown in Fig. 3.(a) is multiplied with the first random phase mask RPM1, shown in Fig. 3.(c), at the input plane. Mask RPM2 and RPM3, shown in Fig. 3.(d) and 3.(e), are laser speckle patterns grabbed using hardware setup. The Fourier transform of the modified input image, i.e. the product of $f(x,y)$ and $M_1(x,y)$, is passed through the combination of random phase masks $M_2(u,v)$ and $M_3(u,v)$ in the Fourier plane. The random phase functions $M_1(x,y)$, $M_2(u,v)$ and $M_3(u,v)$ are chosen to be statistically independent.

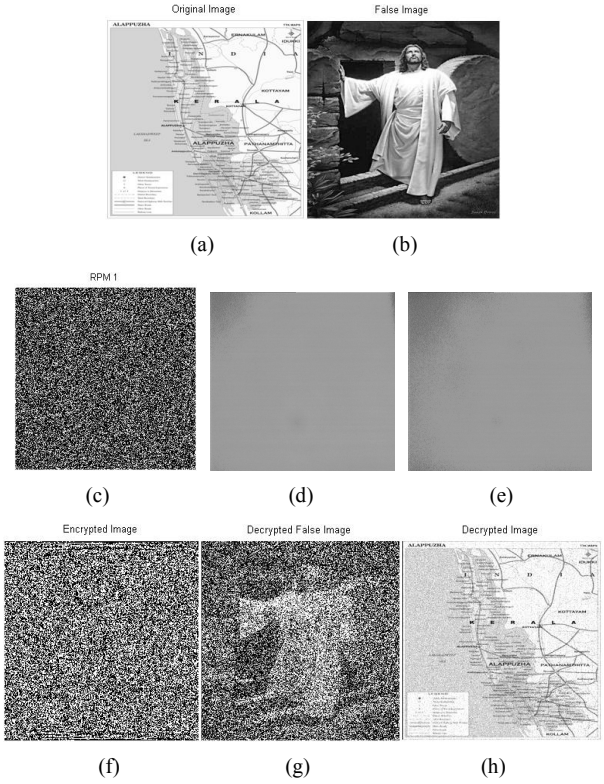

Fig. 3. Simulation results with N×N gray-scale image
(a) Original gray-scale image; (b) False image; (c) Random mask RPM1; (d) Random mask RPM2 (before converting to mask); (e) Random mask RPM3(before converting to mask); (f) Encrypted image; (g) Decrypted false image; (h) Decrypted original image.

IV. CRYPTOGRAPHICAL ENHANCEMENT

Cryptographical enhancement is done which provide an additional security to the system. The cryptographic technique used is derived from the AES cryptosystem. In AES operation there are different stages like substitute bytes, shift rows, mix columns and add round key. Here in this proposed work we are using the shiftrows and mix column operation stage of AES algorithm. In shift row operation the first row of State is not altered. A 1-byte circular left shift is performed in second row; 2-byte circular left shift is performed for the third row, 3-byte circular left shift in the fourth row, and so on. In this paper a slight modified form of shift row operation is done along with an additional shift column operation. Here a random array of numbers are generated according to the size of input image, say if image size is 256×256, then an array of 256 numbers will be generated. Based on the array, first row shifting is done after that column shifting is done so that shifting of rows and columns will be random. For example

a =

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 \\ 8 & 5 & 7 & 9 \end{bmatrix}$$

Random array = [1 4 3 2]

Row shift =

$$\begin{bmatrix} 4 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 \\ 5 & 6 & 7 & 4 \\ 7 & 9 & 8 & 5 \end{bmatrix}$$

Column shift =

$$\begin{bmatrix} 7 & 1 & 4 & 4 \\ 4 & 3 & 7 & 5 \\ 2 & 6 & 8 & 3 \\ 5 & 9 & 2 & 5 \end{bmatrix}$$

Two figures given below the shows a sample operation, where first one is the original figure and second one is the row and column shifter image of first.

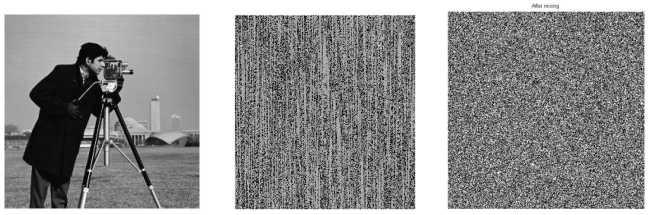

Fig. 4. Cryptographical Enhancement : (a) sample input image (b) enhanced output image (c) simulation output of actual encrypted image image after cryptographical enhancement.

V. SECURITY ANALYSIS

Security analysis can be done by various methods like Mean Square Error (MSE) calculation, statistical analysis, sensitivity analysis, key space analysis, time analysis etc. The security analysis of the proposed image encryption scheme is done using Mean Square Error (MSE) calculation and statistical analysis. Statistical analysis includes histogram analysis and correlation coefficient analysis.

A. Mean Square Error (MSE) Estimation

To evaluate the reliability of the proposed algorithm, Mean Square Error between decrypted image and original image is done. MSE is calculated by using the following relation:

$$MSE = \frac{1}{N \times M}\left[\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left\|\,|fd(x,y)| - |f(x,y)|\,\right\|^2\right]$$

where (N×M) is the size of the image in numbers of pixels. $f_d(x,y)$ and $f(x,y)$ are the decrypted image and the primary image respectively. Instead of N×M matrix, here we are using N×N matrix. The MSE calculated between the decrypted image and the primary image is very small around 10^{-7}.

B. *Statistical Analysis*

Statistical analysis has been successfully used to analyze several ciphers. It can be done mainly in two ways like histogram analysis and correlation coefficient analysis.

a) Histogram Analysis

An image-histogram is a plot which shows how pixels in an image are distributed by graphing the number of pixels at each color intensity level. The resultant histograms after histogram analysis of original image and encrypted one was entirely different so that no one can obtain the actual image from the encrypted. For images we used from USC-SIPI image database and other the encrypted image shows uniform level of histogram. Resultant images are shown below.

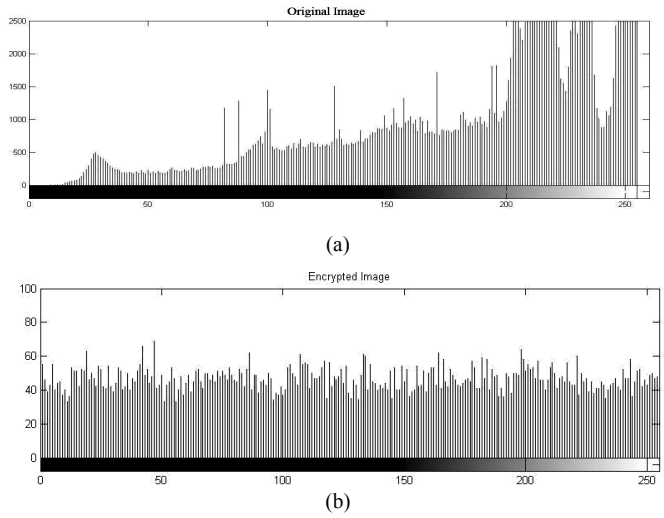

Fig. 5. Histogram Analysis: (a) histogram of original image. (b) histogram of encrypted image

b) Correlation Coefficient Analysis

In addition to the histogram analysis, Correlation coefficient analysis is also added where the correlation between two vertically adjacent and horizontally adjacent pixels are analyzed with several images and their encrypted images. Correlation coefficient is calculated by using the following relation:

$$C_r = \frac{N\sum_{j-1}^{N}(x_j \times y_j) - \sum_{j-1}^{N} x_j \times \sum_{j-1}^{N} y_j}{\sqrt{\left(N\sum_{j-1}^{N} x_j^2 - \left(\sum_{j-1}^{N} x_j\right)^2\right) \times \left(N\sum_{j-1}^{N} y_j^2 - \left(\sum_{j-1}^{N} y_j\right)^2\right)}}$$

where x and y are the value of two adjacent pixels in the image and N is total number of pixels selected from the image. The resultant correlation coefficients are given in Table 1.

	Original image	Encrypted image
Horizontal	0.9917	-0.0052
Vertical	0.9863	-0.0054

Table 1: Correlation coefficients for the two adjacent pixels in the original and encrypted images.

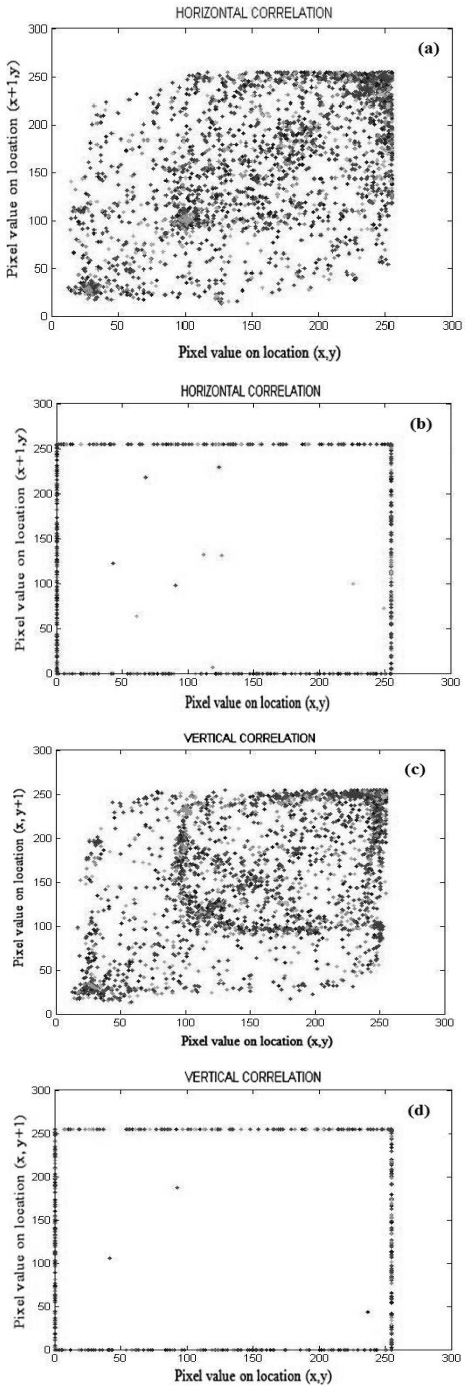

Fig. 6. Correlation of two adjacent pixels: Fig. (a) and (b) respectively, shows the distribution of two horizontally adjacent pixels in the plain and encrypted images. Fig. (c) and (d) respectively, shows the distribution of two vertically adjacent pixels in the plain and encrypted images.

VI. APPLICATION OF ALGORITHM ON IMAGE DATABASE

For extensive study, the algorithm was applied to miscellaneous volume of USC-SIPI image database, which contains four categories of image like textures, aerials, miscellaneous and sequences. Miscellaneous volume contains 16 coloured and 28 monochrome images. Here a few gray scale images are used since the algorithm is only for gray scale. Results are shown in the Table 2.

File		Size	MSE	Correlation coefficient	
Name	Description			Original image	Encrypted image
4.1.01	Girl	256x256	4.8995e-007	0.9616	-0.0104
4.1.05	House	256x256	7.8551e-006	0.9415	-0.0023
4.1.06	Tree	256x256	3.4555e-006	0.9375	-0.0020
4.1.07	Jelly Beans	256x256	9.0983e-006	0.9598	-0.0028
4.2.05	Plane	512x512	5.3735e-007	0.7022	-0.0021
7.1.03	Tank	512x512	8.5992e-008	0.8474	-0.0057
4.2.06	Sailboat	512x512	4.4538e-007	0.9708	0.0017
7.1.08	APC	512x512	2.2229e-006	0.9712	0.0026
Map		900x900	9.3253e-007	0.8494	-0.0102

Table 2. MSE and Correlation coefficient for various images in USC-SIPI image database

VII. CONCLUSION

In this paper, we describe the encryption and decryption of a two dimensional image by using simple Fourier transform and sandwich phase diffuser. The sandwich phase diffuser is made using two laser speckle patterns. After phase diffusion another image is fused to the resultant image and then cryptographical enhancement is done which provide an additional security to the system. The algorithm is simple and at the same time efficient and it provides high security to the image. Simulation results are presented and MSE is calculated between original and encrypted image which is very small.

REFERENCES

[1] A. Kumar, K. Singh, "Elongated laser speckle in imaging of a rough object with slit shaped illumination region: effect of off-axis aberrations", Optik 96. 1994.

[2] N. Towghi, B. Javidi, Z. LuoJ, "Fully phase encrypted image processor", Opt. Soc. Am. A 16. 1995

[3] X. Tan, O. Matoba, T. Shimura, K. Kuroda, B. Javidi, "Secure optical storage that uses fully phase encryption", Appl. Opt. 39. 2000

[4] N.K. Pareek , Vinod Patidar, K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing 24 (2006) 926–934

[5] M. Singh, A. Kumar, "Optical encryption and decryption using a sandwich random phase diffuser in the Fourier plane", Opt. Eng. 46. 2007

[6] Weimin Jin, Caijie Yan, "Optical image encryption based on multichannel fractional Fourier transform and double random phase encoding technique", Optik 118 (2007) 38–41

[7] *Michele De Santis and Giuseppe Schirripa Spagnolo,* "Asymmetric Cryptography as subset of Digital Hologram Watermarking"

[8] M. Singh, et al., "Encryption and decryption using a sandwich phase diffuser made by using two speckle patterns and placed in the Fourier plane: Simulation results", Opt. Int. J. Light Electron. Opt. (2008), doi:10.1016/j.ijleo.2008.03.025

[9] Madan Singh, Arvind Kumar, Kehar Singh, "Encryption by using matrix-added, or matrix-multiplied input images placed in the input plane of a double random phase encoding geometry", Opt Laser Eng (2009)

[10] Narendra Singh, Aloka Sinha, "Gyrator transform-based optical image encryption, using chaos", Optics and Lasers in Engineering 47 (2009) 539–546

[11] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall"