Ewa ŚWIERCZ

Bialystok University of Technology

doi:10.15199/48.2018.02.19

Image encryption algorithms based on wavelet decomposition and encryption of compressed data in wavelet domain

Abstract. *The main purpose of this paper is the evaluation of the developed image encryption algorithm based on wavelet decomposition of images. Encryption algorithms DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are used only for encryption of detail coefficients of the wavelet decomposition and encrypted images are the result of the inverse wavelet transform. Compressed data is also examined in the encryption process. This encryption approach is implemented in Matlab environment.*

Streszczenie. *Głównym celem tego artykułu jest ocena opracowanego algorytmu szyfrowania obrazów opartego o dekompozycję falkową obrazów. Algorytmy szyfrowania DES (Data Encryption Standard) i AES (Advanced Encryption Standard) są wykorzystane do szyfrowania tylko współczynników detali dekompozycji falkowej a zaszyfrowane obrazy są wynikiem odwrotnej transformacji falkowej. Skompresowane dane są również badane w procesie szyfrowania. Ten proces szyfrowania jest implementowany w środowisku Matlab.* ***Algorytmy szyfryzacji obrazu oparte o dekompozycję falkową oraz szyfryzacja skompresowanych danych w dziedzinie transformaty falkowej****.*

Keywords: image cryptosystem, security, wavelet transform, compression**.**
Słowa kluczowe: szyfrowanie obrazu, bezpieczeństwo, transformacja falkowa, kompresja.

Introduction

Devices and services commonly used by people often require safe data transmission and data storage. A digital image is a special type of data. Image transmission is very important in internet communication, multimedia systems, telemedicine, medical imaging systems, military communication, industrial processes, so there is a strong need of special data protection from unauthorized access. Encryption of data, called as cryptography, is a way to ensure a desired safety level. Generally cryptography (encryption and decryption) is the technology encompassing methods of transforming original message into one, that is unintelligible, and then retransforming that message back to its original form. Both encryption and decryption processes are supported by a cryptographic key known only to the sender and the receiver. Additionally encryption and decryption are slow processes and it is often difficult or even impossible to make a secure image in real-time. That is why encryption and decryption algorithms with reduction of time processing are strongly desirable.

Static images are two dimensional (2D) data divided into *N* rows and *M* columns. The intersection of a row and a column is termed a pixel. The value assigned to every pixel is the average brightness of the pixel rounded to the nearest integer value. For video standards static frames can even have *NxM* = 1035x1320 pixels with 16384 grey levels. Colour images have basically three matrices, one matrix for each basic colour in a colour space. So images are data sets of big dimension, what additionally makes an encryption process more difficult. Images have unequally distributed relevant information. It means that only a part of pixels determines some important properties of an image, whereas remaining pixels have less importance and may not provide much information. For this reason images can be decomposed into important and unimportant parts. Some transforms are used as a tool of decomposition of images into important and unimportant parts. Compression algorithms are also able to decompose an image into these two parts [1, 2]. An unimportant part has the meaning only with a connection with an important part. To reduce the overall processing time, only an important part could be selectively encrypted with smaller time of the encryption, while the unimportant part is transmitted in parallel. Such an algorithm can be called a partial encryption. Fig.1 shows the idea of the encryption.

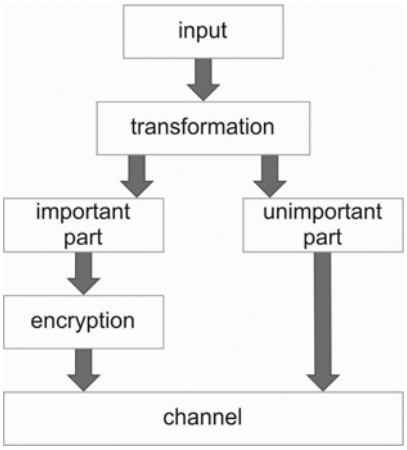

Fig. 1. The proposed approach to secure an image

Algorithms of cryptography – introduction

The DES (Data Encryption Standard) algorithm is the most widely used encryption algorithm [3]. The algorithm works on the 64-bits block of data (block cipher) with the 64-bits key with only 56 bits, which are effective.

Fig. 2. The scheme of encryption (E) and decryption (D): Plaintext (message), Ciphertext (encrypted message)

A cipher means the same thing as a “cryptographic system”. To accomplish encryption, most secret key algorithms use two main techniques known as substitution and permutation. Substitution is simply a mapping of one value to another, whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called rounds.

One round relays on the following operations: 64 bits divided into left and right halves, the right half goes through the function *f*, mixed with the key, the right half added to the left half, halves swapped (except of the last round).

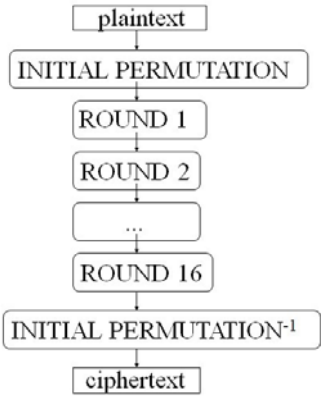

Fig. 3. The simplified scheme of the DES algorithm

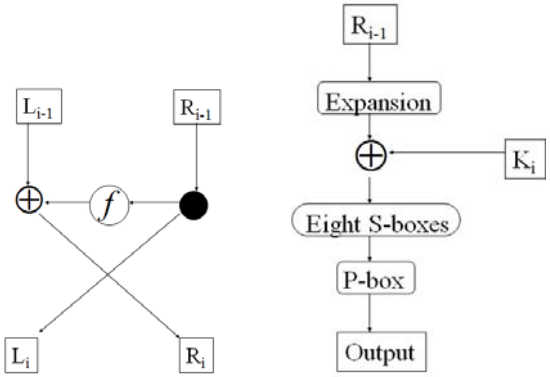

Fig. 4. The operation in one round and details of a single DES round

In the box 'Expansion' the expansion of the right side from 32 to 48 bits is done. Next 48 bits of the key (chosen by schedule) is added. In the 'S-box' each set of 6 bits is reduced to 4. Finally the 'P-box' permutes 32 bits. Equations for the round *i* are the following:

(1) $$L_i = R_{i-1}$$

(2) $$R_i = L_{i-1} \oplus f(R_{i-1})$$

The presented symmetric scheme of the DES algorithm is known as the Fiestel structure, where $\oplus$ denotes the bitwise EXCLUSIVE OR operation. This structure uses the same basic algorithm for both encryption and decryption with the same key. The DES was found to be not as strong as originally believed, so new standards were developed. The algorithm AES (Advanced Encryption Standard) turned out to be a very efficient successor [3]. The algorithm AES with 128-bit blocks is similar to the algorithm DES. The AES allows for three different key lengths: 128, 192, or 256 bits. The main thing that is changed in the AES is a generation of the key schedule from the key. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. Unlike the DES algorithm, the order in which these four steps are executed is different for encryption and decryption. Additionally, the DES algorithm is a bit-oriented cipher whereas the AES algorithm is a byte-oriented cipher. Matlab is a matrix-oriented programming language, perfectly suited for the matrix-based data structure of AES.

Short introduction to wavelet transform of image

2D Discrete Wavelet Transform (2D DWT) is used as a powerful tool for solving different types of image processing problems. 2D DWT can be determined as a set of two matrices of filters, a row and a column one [4, 5]. The first part of decomposition consists of an application of row filters X to an original image I. The column filters Y are used in the next step. This image decomposition is described by (3).

(3) $$C = XIY$$

where I is an original image. In the first level of decomposition of 2D DWT, the image is separated into four parts. Each of them has a quarter size of the original image. They are called approximation coefficients (LowLow or LL), horizontal (LowHigh or LH), vertical (HighLow or HL) and diagonal detail coefficients (HighHigh or HH). A Component LL is a result of low-pass filtering for rows and columns of images, a component LH is a result of low-pass filtering for rows and high-pass filtering for columns, a component HL is a reversed filtering operation to the LH. Finally a component HH is calculated by the high-pass filtering through rows and columns respectively. Approximation coefficients obtained in the first level can be used for the next decomposition level. The scheme of the wavelet decomposition in the level-one is presented in Fig. 5.

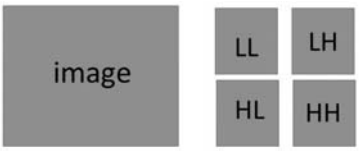

Fig. 5. The level–one decomposition

The Inverse 2D Discrete Wavelet Transform used in image reconstruction is defined by (4)

(4) $$I_{rec} = X^{-1} C Y^{-1}$$

For the orthogonal matrices this formula can be simplified into

(5) $$I_{rec} = X^{T} C Y^{T}$$

where the symbol *T* stands for the transposition operation.

In this paper the wavelet transformation has been chosen for selection of important properties of images, which could be effectively encrypted. Detail coefficients are chosen as an important part of images. Two encryption algorithms, the AES and the DES, are directly used for detail coefficients of the wavelet decomposition, leaving approximation coefficients unchanged [5, 6, 7, 8]. The wavelet transformation with a large set of wavelets, using the concept of multi-resolution analysis, performs decomposition a layer by a layer and gives a lot of possibilities of the choice of transformed data for the encryption task. Additionally, wavelet decomposition allows for easy compression according to the visual characteristics of a human being. This approach leads to increase of a compression ratio and a compression speed with a low binary stream. If the level-one wavelets in Matlab environment are applied to an image, image sub-bands will be produced. This generates coefficient matrices of the level-one approximation (cA1) and horizontal, vertical and diagonal details (cH1, cV1, cD1), respectively. The approximations are the high-scale, low-frequency components of the signal. The details are the low-scale, high-frequency components. Notice that the detail coefficients cD consist mainly of the high-frequency noise, while the approximation coefficients cA contain much less noise than the original signal does.

As previously mentioned, only detail coefficients are assumed as an important part of images and are taken as a message to be selectively encrypted. Approximation coefficients do not come under encryption.

Encryption of detailed coefficients by DES and AES algorithms

Wavelet decomposition of the tested image is presented in Fig. 6. The Matlab function dwt2 is used for the presentation of level-one decomposition with the wavelet bior3.7. Both DES and AES algorithms are used for the assessment of encryption efficiency [5, 6, 7, 8] for detail coefficients. Binary representation of detailed coefficients is achieved by simple conversion from the digital to binary form without sophisticated coding. The image from the file wbarb which resides in the MATLAB directory is taken for analysis. There is an indexed image, which is a matrix containing only integers from 1 to n, where n is the number of colors in the image. The size of the colormap matrix is n-by-3 for an image containing n colors. Next, the wbarb image has been converted to the gray colormap.

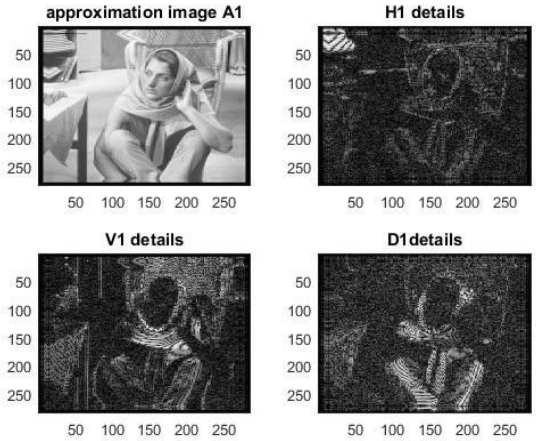

Fig. 6. The wavelet transformation with: 1) the approximation image, 2) horizontal details, vertical details, diagonal details

The Fig. 7 presents the results of the DES encryption algorithm, applied to detail coefficients cH1, cV1, cD1 obtained by the biorthogonal 3.7 wavelet on the level-one decomposition.

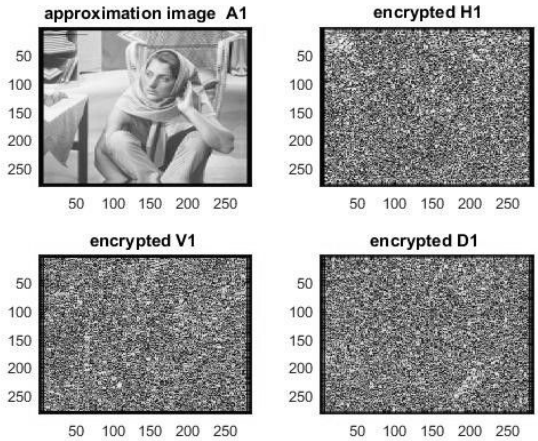

Fig. 7. The DES algorithm for details: horizontal details, vertical details, diagonal details

With the image resolution considered in this paper, encrypted details in the AES algorithm looks similarly for an outside observer. In reality, the result of the AES is substantially different.

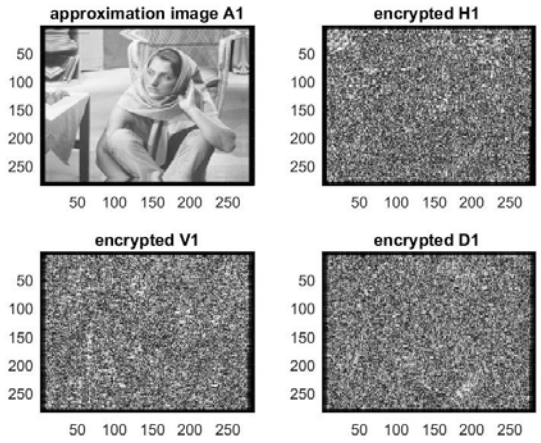

Fig. 8. The AES algorithm for details: horizontal details, vertical details, diagonal details on level-one decomposition

The encrypted image obtained by the inverse wavelet transform, calculated from unchanged approximation coefficients and encrypted details coefficients, presents the distorted original image. When choosing the AES encryption algorithm or the DES encryption algorithm, most of all the security matter should be taken into account [9]. The AES encryption is a more mathematically elegant algorithm and more efficient than the DES cryptographic algorithm and is taken for further experiments.

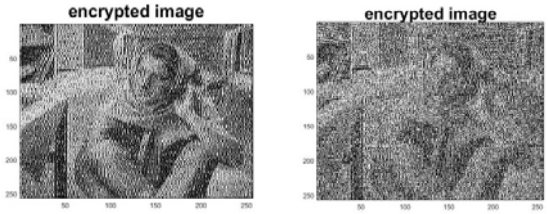

Fig. 9. The encrypted image by the DES and by the AES algorithm with the 128-bit key

Execution time of the DES algorithm in Matlab is 835.83 seconds (Windows 10, 64-bit operating system, RAM 8 GB, Processor Intel, CPU 1.70 GHz) and the absolute error between the original image and the encrypted image is 4.2634e+06, whereas the execution time of the AES algorithm equals only 8.22 seconds and the absolute error between the original image and the encrypted image is 9.0730e+06 and is much bigger than in the DES algorithm. This proves the substantially better security for the AES algorithm. After the decryption technique the original image is retrieved without any errors.

Encryption of a compressed image

Direct encryption of an image with big size in bytes requires a great computational load. The reduction in the size of the file allows more images to be stored in a given amount of a disk or memory space. It also reduces the time required for transmission over a transmitting channel. Compression based on the wavelet decomposition offers higher compression ratios than JPEG or GIF methods for some types of images. The wavelet decomposition can be done as a multilevel process and offers numerous ways for signal analysing [5].

Compression relays on thresholding what means that selected coefficients of the wavelet decomposition will be set to zero when they are less than the threshold (shortly thr). The value of the threshold depends on a chosen design criteria. The threshold which retains more signal's energy after compression is strongly required. On the other hand the threshold controls the distortion level in the

compressed images. If the threshold is higher, then less nonzero coefficients are left and more distortion in compressed images is made. The compression procedure comprises three steps: decomposition, thresholding of detail coefficients and reconstruction from nonzero coefficients remaining after the thresholding process. Approximation coefficients are not taken for compression.

This paper presents a global threshold strategy used in performed experiments. In the Matlab environment also the level thresholding can be chosen. The global threshold is derived from an equal balance between the percentages of retained energy and number of zeros. To compress an image in the Matlab environment, ddencmp and wdencmp functions are used [5]. The function ddencmp provides default values for compression and the function wdencmp makes the actual compression. Output parameters of the function wdencmp called PERF0 and PERFL2 tell, what percentage of the detail wavelet coefficients is set to zero and what percentage of the image's energy is preserved in the compression process, respectively. A lossy compression occurres because a part of coefficients is lost irremediably. After the compression only the AES encryption process is chosen to conduct the encryption process.

As previously, the image from the file wbarb is analysed. For this image the global threshold is thr = 4, PERF0 = 49.80% and PERFL2 = 99.98%, respectively. Because of the smaller number of coefficients after compression (only about 50% coefficients have been left for thr = 4) encrypted images will be of worst quality (more readable for intruders) than encrypted images without compression. Increasing the thr value, the compression ratio rises but the encryption process uses fewer and fewer entries. Execution time for encryption is also shorter. The encryption process becomes less secure than encryption of data without compression and more readable for intruders. There is a conflict between the required high compression ratio and high security of encrypted data, so that encryption and compression should be jointly analysed and performed with reasonable diligence. For this reason additional simple reorganisation of an order of elements flipped left to right is made, what ensures better protection of encrypted images as is shown in experiments presented in this paper.

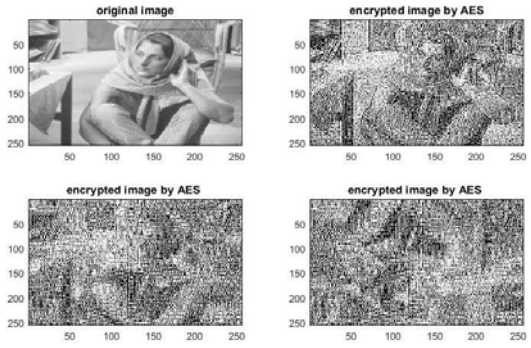

Fig.10. Encrypted images by AES for thr = 4: for only compressed detail coefficients (1,2), for compressed detail coefficients with flipped elements (2,1), for approximation coefficients and compressed detail coefficients with flipped elements (2,2)

Table 1 shows results of compression for an increasing threshold. It is very interesting to notice that percentage of the preserved image energy is very high for analysed values of the threshold, what means that good quality of reconstructed images is expected.

Table.1 Parameters of compression

thr	Time [s]	PERF0 %	PERFL2 %
4	9.1	49.80	99.98
8	7.2	68.06	99.93
16	6.3	79.84	99.80
32	5.8	87.50	99.44

Execution time, jointly for compression and encryption decreases for the increased threshold value. For the thr = 32 only 12.5 percentage of detail nonzero coefficients from level-two decomposition have been left and 99.44 percentage of energy have been preserved. Results of image encryption made by the inverse transform from uncompressed approximation coefficients and compressed detail coefficients with thr = 32 are visible in the following figure:

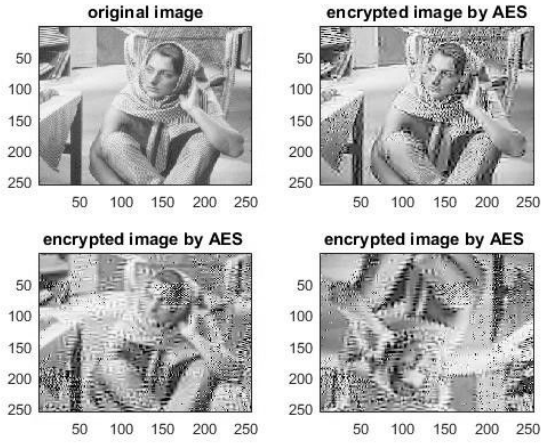

Fig.11. Encrypted images by AES for thr = 32: for only compressed detail coefficients (1,2), for compressed detail coefficients with flipped elements (2,1), for approximation coefficients and compressed detail coefficients with flipped elements (2,2)

Despite many detail coefficients equal to zero, decrypted images seem to be non-distinguishable by human eye from the original image. Encryption and decryption are lossless but losses are introduced only by compression. Lossy compression is generally used for static images, video and sound, where a certain amount of information loss will not be detected by most users. Using lossy compression, the user can decide how much loss to introduce and make a trade-off between the file size and image quality.

Experiments show that high compression requires additional supporting and stronger encryption step. Despite a wide use of the AES algorithm in modern web browsers or in modern email programs, this algorithm should be carefully used in compression applications. Images from reconstruction of a decrypted image and from a compressed image are the same, and they differ from the original image by errors introduced by the compression process. Two of the error metrics used to compare the various image compression techniques are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). The MSE is the cumulative squared error between the compressed and the original image, whereas the PSNR is a measure of the peak error. The mathematical formulae for the MSE and the PSNR are:

$$MSE = \frac{1}{N \cdot M} \sum_{n=1,m=1}^{N,M} (I_{original} - I_{reconstructed})^2 , \quad (6)$$

$$PSNR = 20 \cdot \log 10(255/\sqrt{MSE}) \quad (7)$$

A lower value for the MSE means the lesser error, and as seen from the inverse relation between the MSE and the PSNR, this translates to a high value of the PSNR.

Table 2. MSE errors

thr	MSE
4	3.87
8	12.02
16	31.01
32	69.23

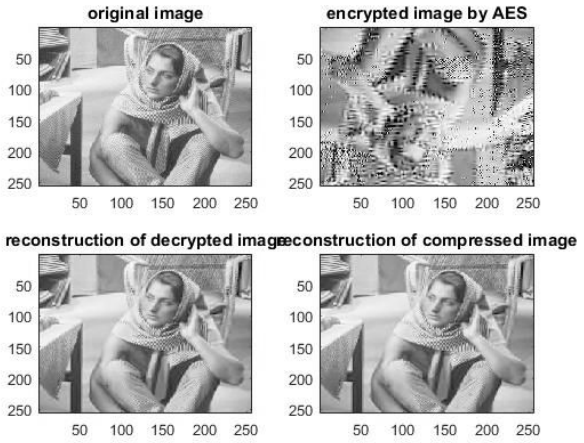

Fig.12. Encrypted and decrypted images by AES for thr = 32: original image (1,1), approximation coefficients and compressed detail coefficients with flipped elements used in encryption (1,2), retrieved image after decryption (2,1), reconstruction from level-two decomposition (2,2)

Conclusion

This paper analyses the capability of encryption of detail coefficients from wavelet decomposition. Detail coefficients of the wavelet decomposition are assumed as an important part of images and are taken as a message to be selectively encrypted. This paper presents only level-two wavelet decomposition. The AES turned out to be superior to the DES, as expected, and only this algorithm is included in experiments. It has been shown that the AES algorithm can be used successfully for encryption in a lossless case but compression performed on detail coefficients gives substantially worse results. Compression leads to a scarce representation of decomposition, and fewer and fewer coefficients take part in encryption. The encryption process becomes less secure than encryption of data without compression and is more readable for intruders. The compressed image contains degradations with respect to the original image, so both processes - compression and encryption should be developed jointly to provide both acceptable degradation and high security.

Acknowledgments. The research was conducted within the project S/WE/1/2015, financially supported by Polish Ministry of Science and Higher Education.

***Author**: Dr hab. inż. Ewa Świercz, Politechnika Białostocka Katedra Telekomunikacji i Aparatury Elektronicznej, ul. Wiejska 45D, 15-351 Białystok, E-mail: e.swiercz@pb.ed.pl.*

REFERENCES

[1] Cheng H., Li X., Partial Encryption of Compressed Images and Videos, *IEEE Transactions on Signal Processing*, 48 (2000), No. 8, 2439-2451

[2] Asid A., Measuring the Strength of Partial Encryption Schemes, *Hewlett Packard Laboratories*, 1501 Page Mill Rd., Palo Alto, CA, USA

[3] Chandrasekhar R.D., Rath A.K., Kabat M.R., Cryptography and network security lecture notes for Bachelor of Technology In Computer Science and Engineering, Veer Surendra Sai University of Technology Burla, Sambalpur, Odisha. https://www.vssut.ac.in/lecture_notes

[4] Yu Z., Zhe Z., Haibing Y., Wenjie P., Yunpeng Z., A Chaos-Based Image Encryption Algorithm Using Wavelet Transform, *2nd International Conference on Advanced Computer Control,* vol.2 pp. 217-222, Shenyang, China, 27-29 March 2010

[5] Misiti M., Misiti Y., Oppenheim G., Poggi J.M., User's Guide: Wavelet Toolbox for use with MATLAB Mathworks R2015b

[6] Werner M., Przegląd, analiza, i implementacja w środowisku Matlab agorytmów szyfrowania sygnałów, *praca magisterska,* Politechnika Białostocka, Białystok 2014

[7] http://www.mathworks.com/matlabcentral/fileexchange/37847-data-encryption-standard-des

[8] http://www.mathworks.com/matlabcentral/linkexchange/links/3025-aes-advanced-encryption-standard

[9] Parthasarathy M.B, Srinivasan B., Increased Security in Image Cryptography using Wavelet Transforms, *Indian Journal of Science and Technology*, 8(2015), No.12, 1-8