IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by
Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science, Engineering&Technologies" RASET-2015

Research Paper

SUDOKU BASED IMAGE SECURITY ALGORITHM

P Pavithra[1]*, P Suguna[1] and K Punithagayathri[1]

Corresponding Author:* ***P Pavithra*

In this paper introduces the Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it.The embedding order based on the order key of which is stored with cover in a database table in both the sender and receiver sender. a new effective and lossless image encryption algorithm using a Sudoku Matrix to scramble andencrypt the image. The new algorithm encrypts an image through a three stage process. In the first stage, a referenceSudoku matrix is generated as the foundation for the encryption and scrambling processes. The image pixels' intensitiesare then changed by using the reference Sudoku matrix values, and then the pixels' positions are shuffled using theSudoku matrix as a mapping process. The advantages of this method is useful for efficiently encrypting a variety ofdigital images, such as binary images, gray images, and RGB images without any quality loss.

Keywords: Steganography, Scrambling algorithm, DCT compression

INTRODUCTION

In the present electronic communication scenario, data security is one of the major challenges. After the World WarII, the need for a secure and robuscommunication between the communicating entities has increased due to the fearof terrorism. Steganography is*concealed writing* and is the scientific approach of inserting the secret data within a cover media such that theunauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which issent from transmitter to receiver without scrambling. Image compression can be lossy or lossless [4, 5]. In a lossless compression algorithm, compressed data can be used to recreate an exact replica of the original; no information is lost to the compression process. This type of compression is also known as entropy coding. In lossy compression, the original signal cannot be exactly reconstructed from the compressed data. The reason is that, much of the detail in an image can be discarded without greatly changing the appearance of the image. As an example consider an image of a tree, which occupies several

[1] KPR Institute of Engineering and Technology, Coimbatore.

hundred megabytes. In lossy image compression, though very fine details of the images are lost, but image size is drastically reduced. Lossy image compressions are useful in applications such as broadcast television, videoconferencing, and facsimile transmission, in which a certain amount of error is an acceptable trade-off for increased compression performance. Methods for lossy compression include: Fractal compression, Transform coding, Fourier-related transform. In this paper, we introduce a new image encryption scheme based on the Sudoku Matrix. Instead of using an unfinishedSudoku Puzzle, which is employed by previous Sudoku based encryption algorithm, we used the full solution to aSudoku Puzzle, i.e. a Sudoku matrix to encrypt the image directly. In addition, we broadened the conception of theSudoku matrix from 9 by 9 to any N by N matrix, where N is some square number. Our algorithm also employs a 1DChaotic Logistic Map to generate a random-like Sudoku Matrix and it is used as our reference matrix. By changing thepixels' values according to the Sudoku reference matrix, the histogram after encryption is dramatically changedcompared to the original one. Furthermore, with the property of the Sudoku matrix that no two digits in the same blockcan be aligned in the same row, column or box, the input image can be scrambled to a desired output. Therefore, no twopixels originally in the same block will be in the same row, or the same column or the same box in the output.The presented algorithm can be used to encrypt other types of images such as color images, gray images, binary imagesand etc. The security key is selective and has a very large number space.

STEGANOGRAPHY

In the present electronic communication scenario, data security is one of the major challenges. After the World War II, the need for a secure and robust communication between communicating entities has increased due to the fear of terrorism. The publishers of digital audio and video are worried of their works being corrupted by illegal copying or redistribution, hence it is of primary importance to protect information Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. n. Cover image is known as carrier image and is the original image in which the secret data ie., the payload is embedded. The unified image obtained after embedding the payload into the cover image is called the stego image. Image Steganography includes several techniques of hiding the payload within the cover image. The most popular hiding techniques are Spatial Domain based Steganographic Techniques and Transform Domain based Steganographic Techniques.

Mean Square Error (MSE): It is defined as the square of error between cover image and stegoimage. The distortion in the image can be measured using MSE.

Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e., it measures the statistical difference between the cover and stegoimage

Cover Image: The cover image is color or gray scale of any size and format. If the cover image is color then convert into gray scale image and corresponding pixel intensity values.

Stegoimage: It is an unified image obtained by the combination of the payload and cover image.

Pixel Management: The gray scale cover image pixel intensity vary from zero to 255. During the payload embedding process the intensity values of cover image may exceed lower and higher level limits which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper 240 instead of zero and 255.

Segmentation: The cover image is segmented into 8x8 matrices. The DCT is applied on each 8x8 block to get DCT coefficients which are used to hide the payload Most Significant Bit (MSB) based on the DCT coefficient values of the cover image.

DCT Based Steganography Algorithm to embed image:

Step 1: Read cover image.

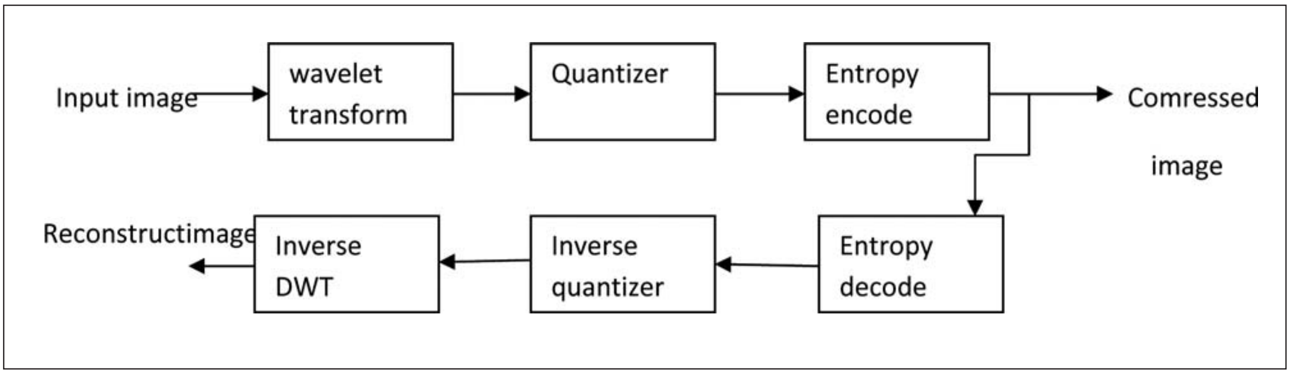
Step 2: Read secret message and convert it scrambled image.

DISCRETE WAVELET TRANSFORM

Wavelets are signals which are local in time and scale and generally have an irregular shape. A wavelet is a waveform of effectively limited duration that has an average value of zero. The term 'wavelet' comes from the fact that they integrate to zero; they wave up and down across the axis. Many wavelets also display a property ideal for compact signal representation: orthogonality.

Image compression is a key technology in transmission and storage of digital images because of vast data associated with them. This research suggests a new image compression scheme with pruning proposal based on discrete wavelet transformation (DWT). Image compression is important for many applications that involve huge data storage, transmission and retrieval such as for multimedia, documents, videoconferencing, and medical imaging. Uncompressed images require considerable storage capacity and transmission bandwidth. The objective of image compression technique is to reduce redundancy of the image data in order to be able to store or transmit data in an efficient form. This results in the reduction of file size and allows more images to be stored in a given amount of disk or memory space.

The compression features of a given wavelet basis are primarily linked to the relative scarceness of the wavelet domain representation



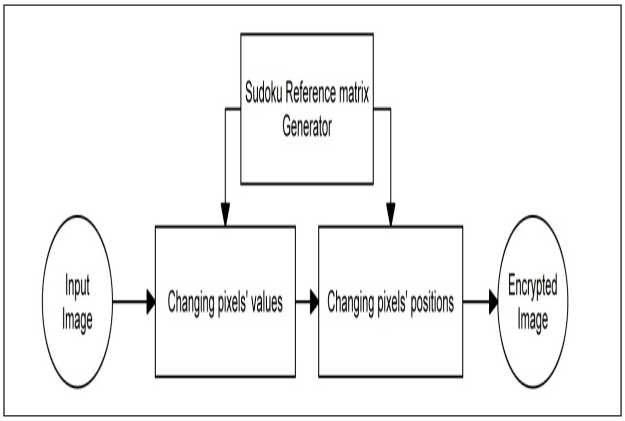
for the signal. The notion behind compression is based on the concept that the regular signal component can be accurately approximated using the following elements: a small number of approximation coefficients (at a suitably chosen level) and some of the details coeffients.

SUDOKU MATRIX

Sudoku Matrix using a new effective and lossless image encryption algorithm to scramble and encrypt the image. The new algorithm encrypts an image through a three stage process.

IMAGE ENCRYPTION USING THE SUDOKU MATRIX

In this section a novel encryption scheme using the Sudoku Matrix. The basic steps are provided. Block diagram for Image Encryption Scheme.

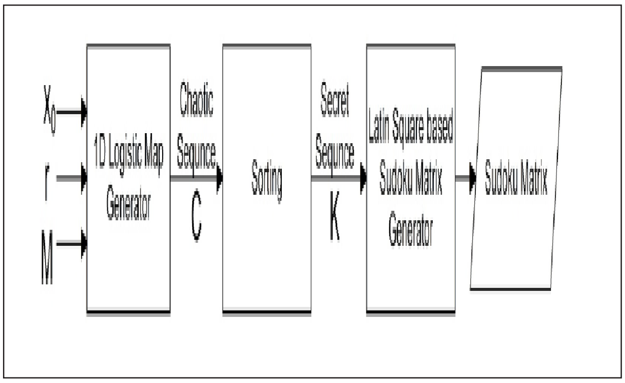


The entire algorithm could be divided into three main stages: generating the Sudoku Reference Matrix, changing Pixels' values and changing pixels' positions. The whole encryption process can be described as follows: first, a Sudoku Reference Matrix **Ref** is generated and then the input image is resized to match the size of **Ref**. Then, the input image's pixel values are changed according to the **Ref** matrix. Finally, the input image's pixel positions are also shuffled according to the **Ref** matrix. The decryption process is simply the reverse of the encryption process. A security KEY is used to generate Sudoku Reference Matrix **Ref**. We decrypt an encrypted image by first changing the positions of image pixels and then changing pixels' value according to the **Ref** matrix. Finally we obtain the decrypted image as the output.

STAGE:1

Generating the Sudoku Reference matrix: the flow chart of the Sudoku Reference matrix Generator:

Flow chart of the Sudoku Reference matrix Generator


X_0
r
M
1D Logistic Map Generator
Chaotic Sequence
C
Sorting
Secret Sequence
K
Latin Square based Sudoku Matrix Generator
Sudoku Matrix

Generating a Chaotic Sequence C using a Logistic Map

In the inputs determines the initial value for the logistic map while *M* determines the length of the Chaotic Sequence **C**. The definition of a discrete Logistic map is as follows

X(n+1)=r.xn.(1-xn) . It is clear to see that once (x0,r) are given, the whole chaotic sequence is determined.

GENERATING THE SUDOKU MATRIX

First of all, we present the algorithm for generating a Latin square using a ring shift method. The input is a sequence of numbers **B** with length *M* and the output is a Latin square **L** with size *M* by *M*.

Sub Latin square#1 Sub Latin square#2 Sub Latin square#3

L= Sub Latin square#2 Sub Latinsquare#3 Sub Latin square#

Sub Latin square#3 Sub Latin square#1 Sub Latin square#2

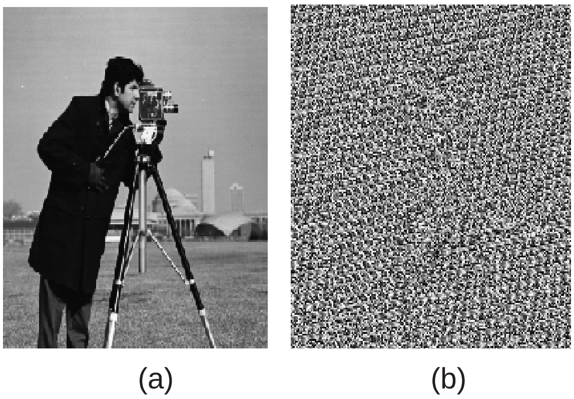
STAGE 2:

Changing image data values using a Sudoku Matrix

Pixels' intensities or values in a digital image carry abundant information. For example, the brightness and contrast are closely related to the pixels' intensity in an image, and they are crucial for identifying the objects. Therefore, we can encrypt a digital image by changing its data values. In reality, it is expected to see a very different histogram of the encrypted image from the original one. And the ideal output histogram follows a uniform distribution.

Firstly, the Sudoku **Ref** matrix subtracts 1 such that its possible values become [0, 1, 2, …, N-1] and then it is rescaled, such that the numbers [1, 2, …,N] now are replaced by [0, 255/(N+1),…, 255*(N-1)/(N+1)] respectively. The original image is padded/resized to fit the size of the Sudoku **Ref** such that the new image could be divided exactly *R* integer blocks. This new image will be used for the future processing. Later on, the input image is processed block by block. For each block, the operation of Mod(X+Y,255) is applied, where X is some selected block in the input image and Y is the rescaled **Ref** matrix. Figure shows the differences between before and after applying the proposed algorithm. Changing image pixel values using a Sudoku Reference matrix

(a) Cameraman Image; (b) Image of after changing pixels' value;



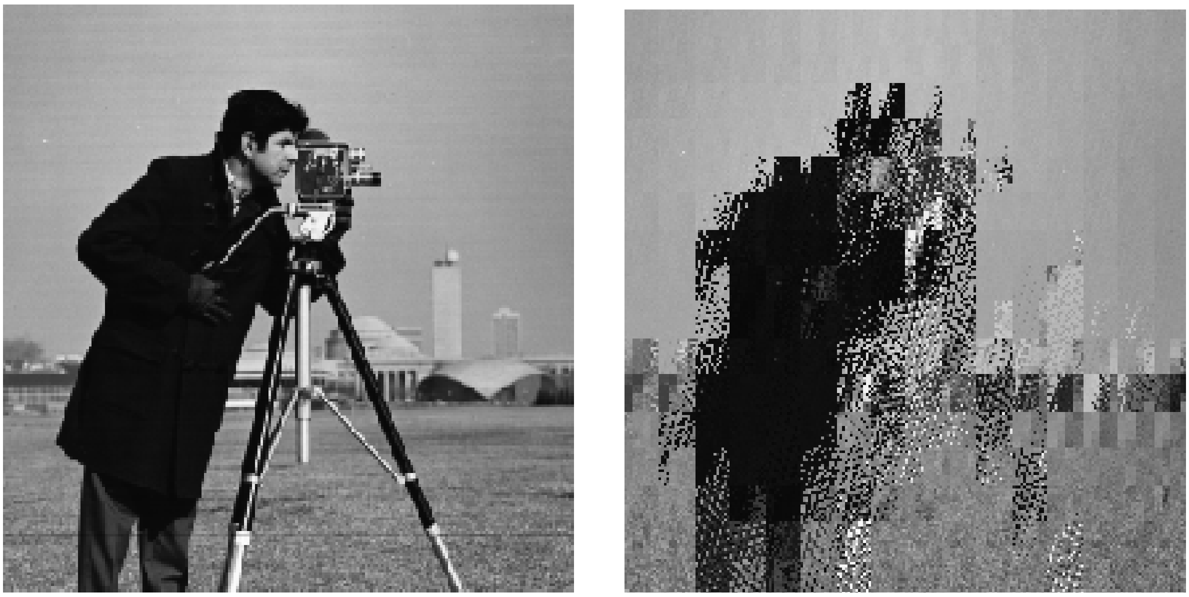
STAGE 3:

Changing image data positions using a Sudoku Matrix

A shuffling algorithm can be expressed as a mapping function ***f***, such that ˆ(x,y),• Iwhere (X,Y) is the (row, column) pair for some pixel in image I, ´(r,c), =f(x,y), where (r,c)is the new (row, column) pair for the input pixel after shuffling. The mapping function ***f*** has to be a one-to-one and onto function. In addition, if we do not want to change the image size after shuffling then ***f*** has to be a self-map function as well. Here the 'self-map' property guarantees the domain and the range of ***f*** are the same, 'one-to-one' and 'onto'property impose the one to one corresponding between the domain and the range.In any Sudoku reference matrix **Ref**, the mapping relationship between (row, column) pair and (block, digit) pair is a self-map and bijective (both one-to-one and onto) function. Therefore,this relationship can be also used for shufflingimage and we call this mapping a Sudoku mapping.

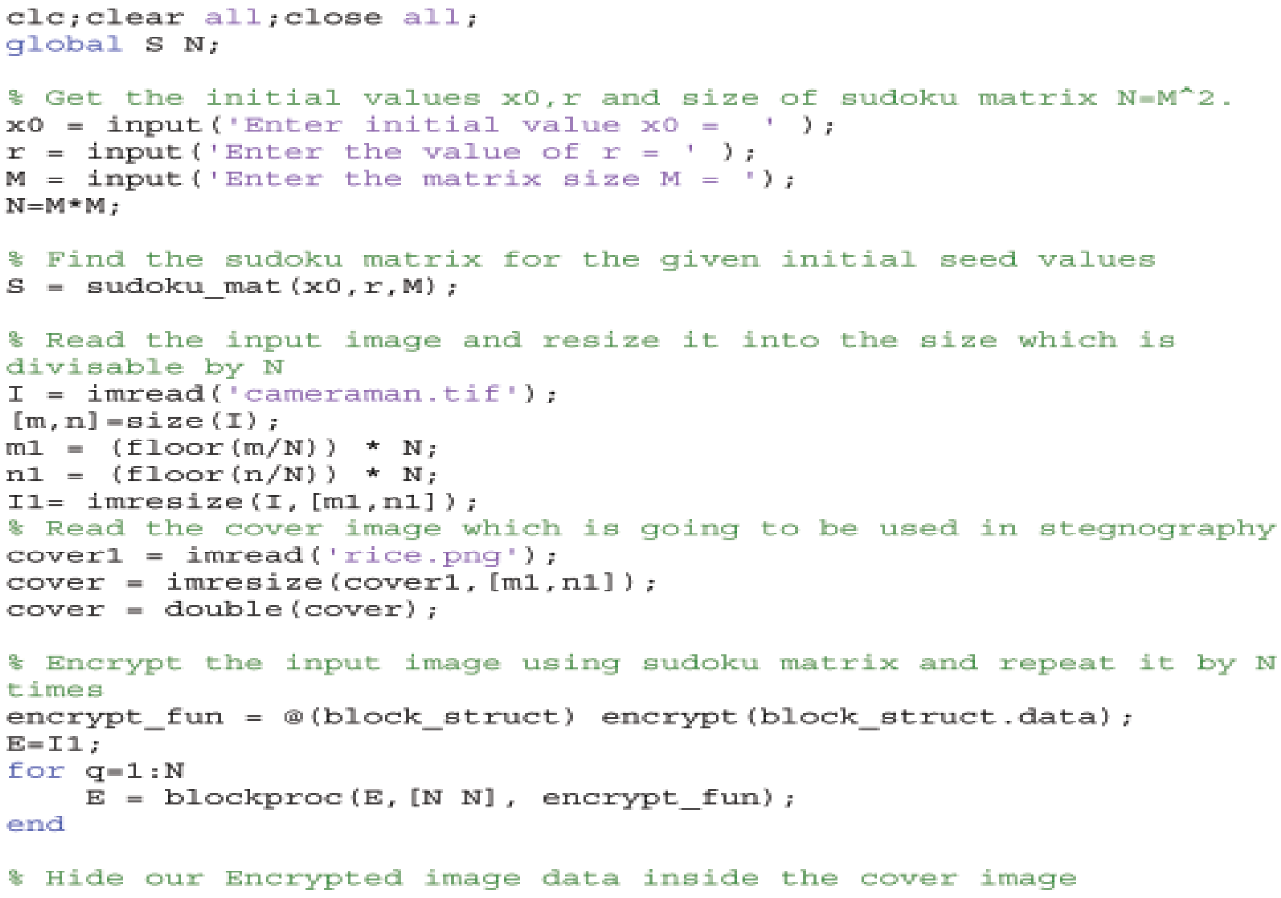
Sudoku mapping (x,y)=(r,c) Shuffling image using the Sudoku Mapping with iterative process

(a) Original Image; (b) Ref size 16 by 16, #iteration = 1, d = 0.4830

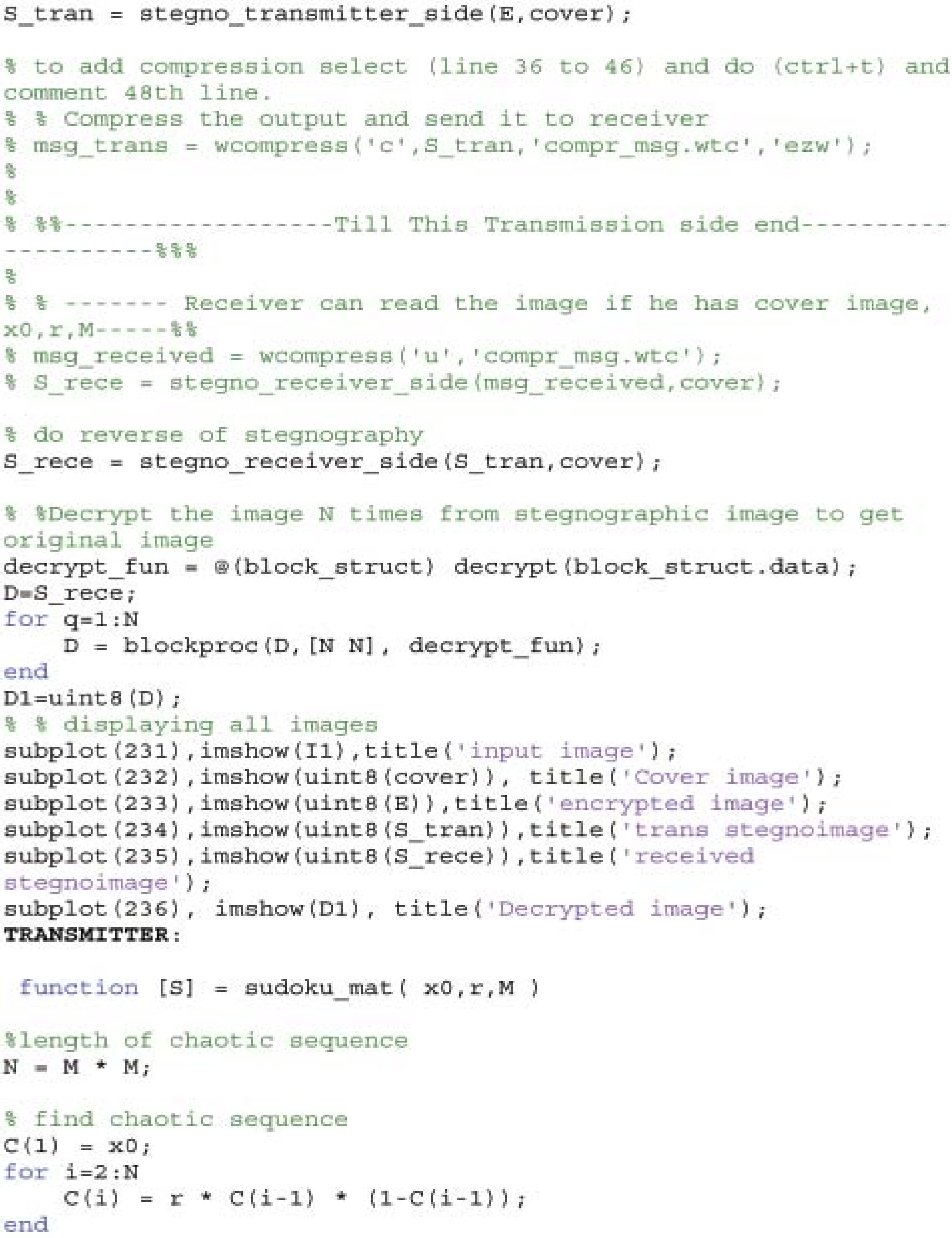


(a) (b)

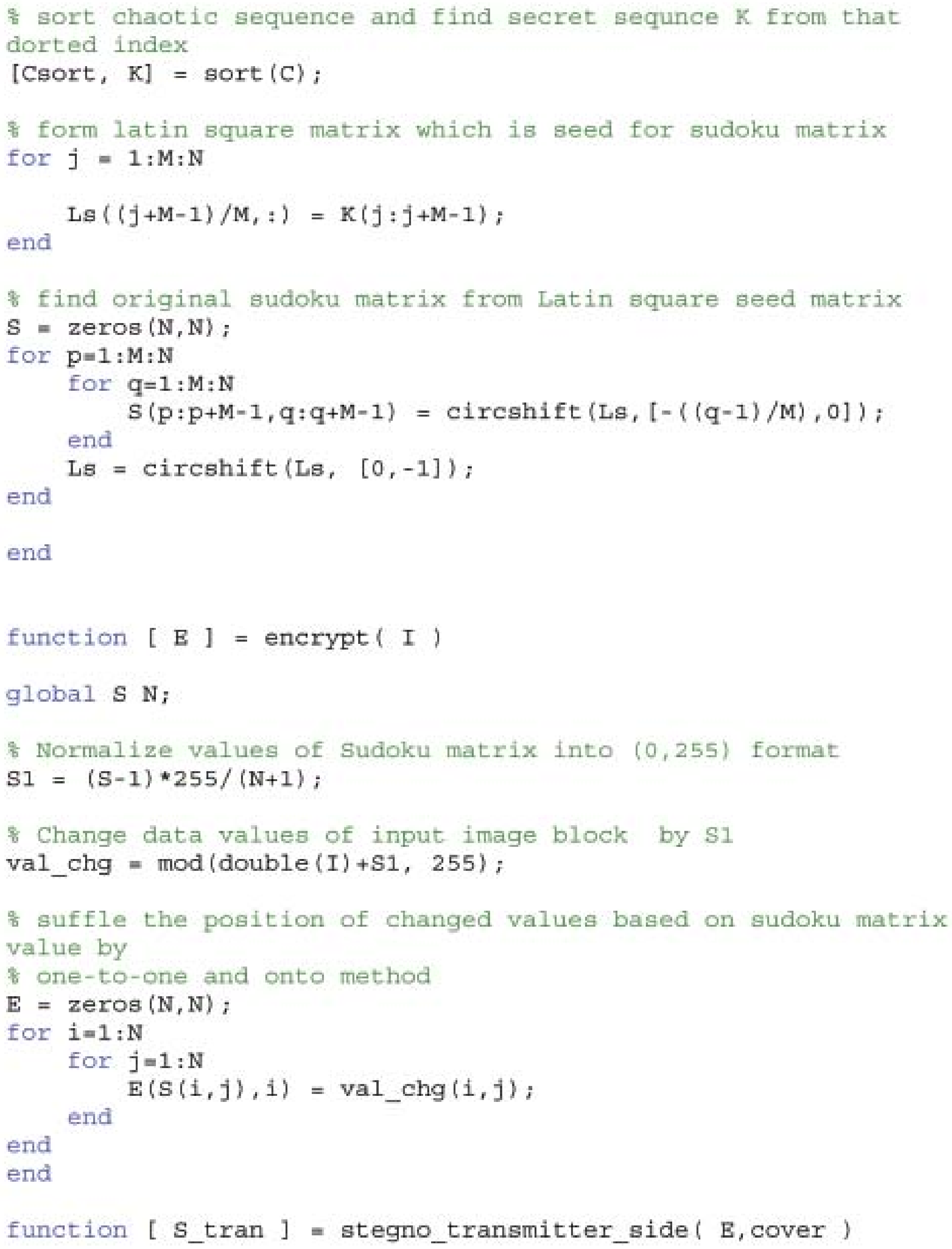
IMAGE PROCESSING USING SIMULATION



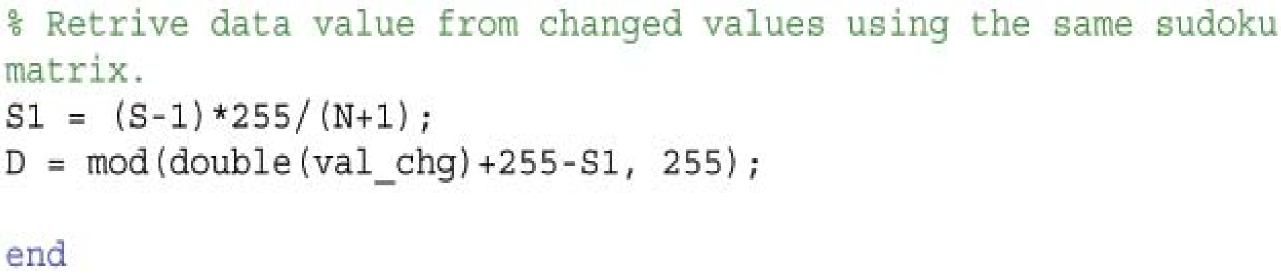
```
clc;clear all;close all;
global S N;

% Get the initial values x0,r and size of sudoku matrix N=M^2.
x0 = input('Enter initial value x0 =  ' );
r = input('Enter the value of r = ' );
M = input('Enter the matrix size M = ');
N=M*M;

% Find the sudoku matrix for the given initial seed values
S = sudoku_mat(x0,r,M);

% Read the input image and resize it into the size which is
divisable by N
I = imread('cameraman.tif');
[m,n]=size(I);
m1 = (floor(m/N)) * N;
n1 = (floor(n/N)) * N;
I1= imresize(I,[m1,n1]);
% Read the cover image which is going to be used in stegnography
cover1 = imread('rice.png');
cover = imresize(cover1,[m1,n1]);
cover = double(cover);

% Encrypt the input image using sudoku matrix and repeat it by N
times
encrypt_fun = @(block_struct) encrypt(block_struct.data);
E=I1;
for q=1:N
    E = blockproc(E,[N N], encrypt_fun);
end

% Hide our Encrypted image data inside the cover image
```



```
S_tran = stegno_transmitter_side(E,cover);

% to add compression select (line 36 to 46) and do (ctrl+t) and
comment 48th line.
% % Compress the output and send it to receiver
% msg_trans = wcompress('c',S_tran,'compr_msg.wtc','ezw');
%
%
% %%------------------Till This Transmission side end----------
----------%%%
%
% % ------- Receiver can read the image if he has cover image,
x0,r,M-----%%
% msg_received = wcompress('u','compr_msg.wtc');
% S_rece = stegno_receiver_side(msg_received,cover);

% do reverse of stegnography
S_rece = stegno_receiver_side(S_tran,cover);

% %Decrypt the image N times from stegnographic image to get
original image
decrypt_fun = @(block_struct) decrypt(block_struct.data);
D=S_rece;
for q=1:N
    D = blockproc(D,[N N], decrypt_fun);
end
D1=uint8(D);
% % displaying all images
subplot(231),imshow(I1),title('input image');
subplot(232),imshow(uint8(cover)), title('Cover image');
subplot(233),imshow(uint8(E)),title('encrypted image');
subplot(234),imshow(uint8(S_tran)),title('trans stegnoimage');
subplot(235),imshow(uint8(S_rece)),title('received
stegnoimage');
subplot(236), imshow(D1), title('Decrypted image');
TRANSMITTER:

 function [S] = sudoku_mat( x0,r,M )

%length of chaotic sequence
N = M * M;

% find chaotic sequence
C(1) = x0;
for i=2:N
    C(i) = r * C(i-1) * (1-C(i-1));
end
```

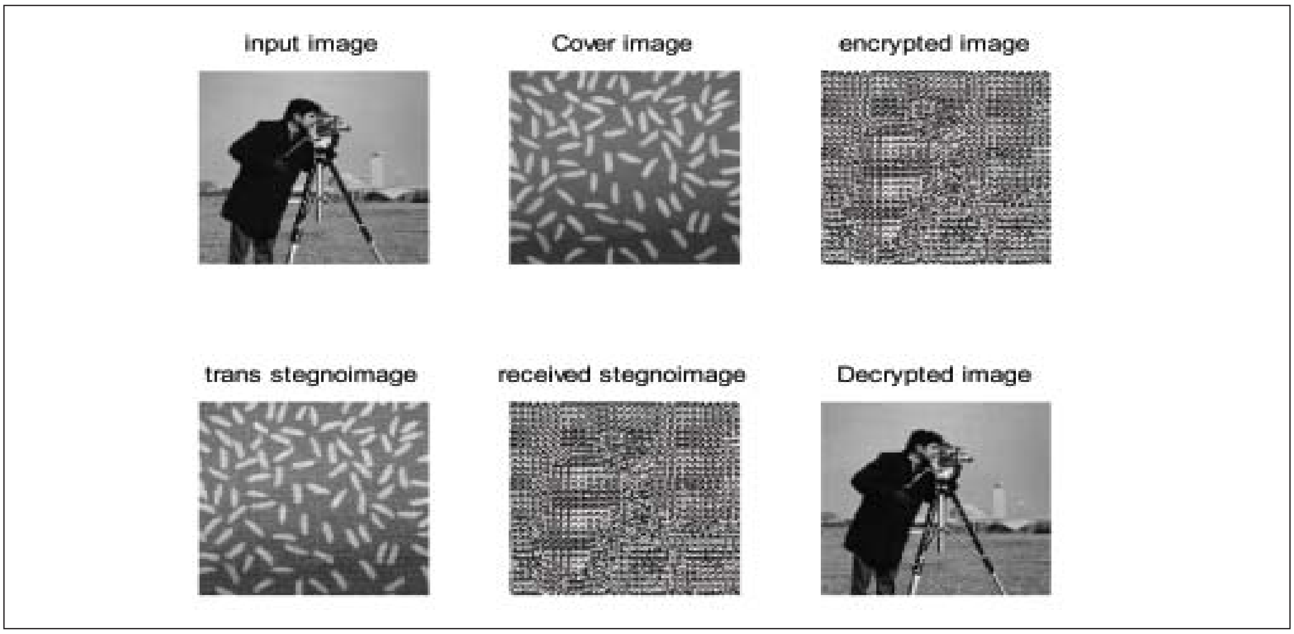


```
% sort chaotic sequence and find secret sequnce K from that
dorted index
[Csort, K] = sort(C);

% form latin square matrix which is seed for sudoku matrix
for j = 1:M:N

    Ls((j+M-1)/M,:) = K(j:j+M-1);
end

% find original sudoku matrix from Latin square seed matrix
S = zeros(N,N);
for p=1:M:N
    for q=1:M:N
        S(p:p+M-1,q:q+M-1) = circshift(Ls,[-((q-1)/M),0]);
    end
    Ls = circshift(Ls, [0,-1]);
end

end


function [ E ] = encrypt( I )

global S N;

% Normalize values of Sudoku matrix into (0,255) format
S1 = (S-1)*255/(N+1);

% Change data values of input image block  by S1
val_chg = mod(double(I)+S1, 255);

% suffle the position of changed values based on sudoku matrix
value by
% one-to-one and onto method
E = zeros(N,N);
for i=1:N
    for j=1:N
        E(S(i,j),i) = val_chg(i,j);
    end
end
end

function [ S_tran ] = stegno_transmitter_side( E,cover )
```



```
% Retrive data value from changed values using the same sudoku
matrix.
S1 = (S-1)*255/(N+1);
D = mod(double(val_chg)+255-S1, 255);

end
```

SIMULATION OUTPUT



REFERENCES

1. Dang P P and Chau P M (2000), "Image encryption for secure Internet multimedia applications," Consumer Electronics, *IEEE Transactions on,* Vol. 46, No. 3, pp. 395-403.
2. Tang L (1996), "Methods for encrypting and decrypting MPEG video data efficiently", ACM, Boston, Massachusetts, United States.
3. Kumar V and Kumar D (2010), "Performance Evaluation of DWT Based Image Steganography," *IEEE International Conference onAdvance Computing,* pp. 223-228.
4. Weiqi Luo, Fangjun Huang, and Jiwu Huang. (2010): "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEETransactions on*
5. Kharate G K, Pati V H (2010), "Color Image Compression Based On Wavelet Packet Best Tree", *International Journal of Computer Science*, Vol. 7, No. 3.
6. Haque M R and Ahmed F (2005), "Image data compression with JPEG and JPEG2000", 8th International Confrrence on Computer and Information Technology, pp. 1064-1069.

IJERST

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com

ISSN 2319-5991
01
9 772319 599001