RESEARCHERID
THOMSON REUTERS

[Khan* *et al.*, 7(8): August, 2018]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IMAGE ENCRYPTION USING TRAPDOOR ONE WAY FUNCTION

Eshan Khan [*1], Deepti Rai [2]
[*] Department of EC, AIT, Ujjain, India

DOI: 10.5281/zenodo.1403406

ABSTRACT

In this paper introduction about the digital images and digital image processing is given. In every application of digital image processing highly encrypted and adaptive algorithm is needed. For the encryption and decryption of the images an adaptive pixel masking technique is used in our paper. For removing noises which affect the images during processing with the help of Linear and Space invariant filters. At long last the execution of the proposed image encryption-decryption calculation working in conjugation with the image restoration system has been assessed regarding PSNR and MSE.

KEYWORDS: Trapdoor Function, Peak Signal to Noise Ratio, Mean Square Error, Wiener Filter.

1. INTRODUCTION

Image encryption is crucial for the quantity of advanced image applications. There are different encryption systems for image encryption. As image quality debases at an exceptionally fast rate, if the encryption mechanism change the pixel arrangement then it influences the inventiveness of the image. Further, noise additionally influences the image quality. Consequently we need to outline a proficient encryption-decryption algorithm and also noise evacuation mechanism. An image can be characterized as an element of two measurements f(x,y) where x and y are spatial co-ordinates. The intensity of the image is a component of the co-ordinates (x,y) any point of x and y. On the off chance that it is along these lines, the estimations of (x, y), and the gray level [f(x, y)] are discrete and finite values, at that point it is known as an digital image. In this way we can state that digital image is a numeric representation of (normally binary) a two-dimensional image. On the off chance that the image determination is settled, it might be named vector or raster type.

2. MATERIALS AND METHODS

Image Encryption using Trapdoor one way function

The Encryption Mechanism is outlined utilizing Trapdoor Function clarified beneath:

The trapdoor or one way functions are arrangements of mathematical formulas which demonstrate the accompanying properties:

$y_{img} = g(x); is\ easy\ to\ calculate\ realtively$ (i)

$x = g^{-1}(y\_img) is\ generally\ iinfeasible\ without\ additional\ information$ (ii)

Examples of trapdoor functions are modular functions and bit-xor functions.

Noise Attacks on Images

In spite of the fact that there can be a plenty of degradations that can influence the images to be encrypted and decrypted, yet the ones that are the most widely recognized and can be modelled are:

1) Gaussian Noise: It's a kind of noise that displays a flat noise power spectral density bend over an extensive scope of frequencies that are contained in the image.

Mathematically:

$\frac{K_0}{2}(psd) = CONSTANT$ (iii)

Here,

$\frac{K_0}{2}(psd)$ represents the noise power spectral density of the Gaussian Noise Process.

CONSTATNT is the value over the ranges of frequency

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Image Restoration Process

The image denoising component ought to have the accompanying two characteristics:

1) Linearity: This property is a mix of two unique properties v.i.z. Additivity which can be scientifically expressed as:

$Z1 \xrightarrow{T} L1$ (iv)

$Z2 \xrightarrow{T} L2$ (v)

$\alpha.Z1 + \beta.Z2 \xrightarrow{Trans} L1 + L2$ (vi)

Here,
Z1 is input 1
Z2 is input 2
L1 is input 1
L2 is input 2
Trans is transformation done by the system
α and β are system constants
The homogeneity principle states:

$Z1 \xrightarrow{T} L1$ (vii)

$a.Z1 \xrightarrow{T} k.L1$ (viii)

Here,
a is a system constant

2) Space Invariance: This property indicates that the properties of the system don't change with spatial coordinates

$G(x, y - Sht) \xrightarrow{H} X(x, y - Sht)$ (ix)

Here,
$G(x, y - T)$ represents shift
(x,y) are the coordinates of image pixels
H is the system function.
A Wiener filter is a close approximation of the space invariance and linear filtering model.

Proposed Methodology

The proposed procedure utilized for the design of the encryption calculation and consequent image rebuilding is clarified in detail underneath:

1) Load and Display image of interest.
2) Obtain the information of Pixel and Size.
3) Create Key contingent on Pixel and Size data.
4) Create Encrypted Image contingent on Pixel and Size data and Key.
5) Design the Model of Image Degradation by characterizing the factual estimations of the blurring and noise impacts.
6) Image display with Degradations
7) Apply filtering by degradation statistical parameters accepting zero NSR
8) Apply filtering by degradation statistical parameters with evaluated NSR
9) De-noise Image and show it
10) Decrypt image utilizing Key and Decryption calculation
11) Compute Evaluation Parameters, for example, Mean Square Error, PSNR and Throughput

Performance Metrics

The performance is decided based on:

$PSNR = 10log size^2 / \frac{1}{i*j}\sum_{i,j}^{m,n}(I - I')^2$ (xi)

Here,
I is the x-pixels
J is the y-pixels
I is the image under interest
I' represents image after process

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

$MSE = \frac{1}{i*j}\sum_{i,j}^{m,n}(I - I')^2$ (xii)

Here,
I is the x-pixels
J is the y-pixels
I is the image under interest
I' represents image after process

3. RESULTS AND DISCUSSION

The results are given below:
We have used Two test images i.e. lena.jpg and cameraman.jpg in this case.

Fig.1 Test Image1 (lena.jpg)

Fig.2 Test Image2 (cameraman.jpg)

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

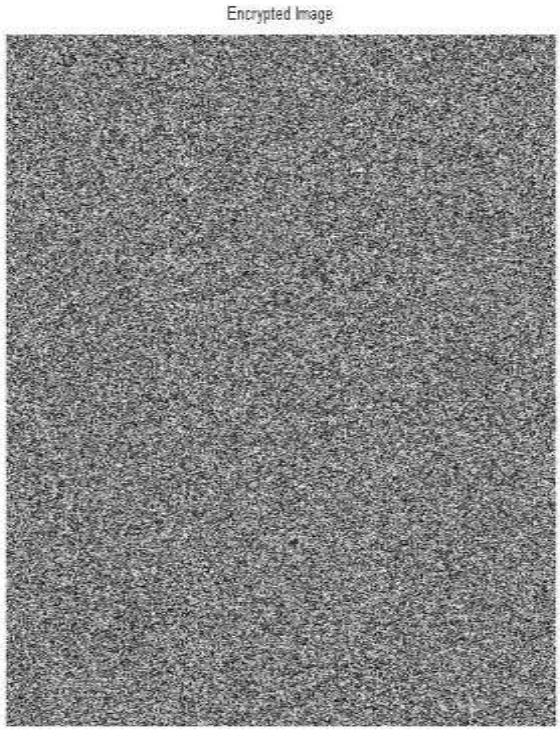

Fig.3 Encrypted Image using Proposed Methodology

Fig.4 Image undergoing Blurring Effect

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Fig.5 Image undergoing Blurring and Gaussian Noise attack

Fig.6 Image restoration with parameter NSR being zero

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Fig.7 Image restoration with estimated NSR

Table 1. Comparison table for PSNR for lena.jpg

NOISE TYPE	PSNR
Gaussian	75.35
Salt and Pepper	78.84
Speckle	80.14
Poisson	83.52

Table 2. Comparison table for PSNR for cameraman.jpg

NOISE TYPE	PSNR
Gaussian	74.38
Salt and Pepper	71.02
Speckle	76.95
Poisson	79.56

4. CONCLUSION

It can be finished up from the outcomes and past discourses that the proposed strategy accomplishes higher measure of arbitrariness because of versatile pixel masking. Additionally the impacts of different noise impacts have been expelled utilizing direct and space invariant filtering. It can be completely watched that the proposed method accomplishes higher estimations of Peak Signal to Noise Ratio contrasted with past systems. It can likewise be noticed that the lesser the estimation of MSE, the higher the estimation of PSNR. This approves the outcomes along the work acquired. At long last a higher estimation of throughput contrasted with standard encryption calculations imply the way that the proposed calculation does not have over the excessive space and time complexity in this way making it able and proper for commonsense applications and executions.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

REFERENCES

[1] Faiq Gmira, Said Hraoui, Abderrahim Saaidi, Abderrahamane Jarrar, "Securing the Architecture of the JPEG Compression by an Dynamic Encryption", IEEE ,2015.
[2] Reversibility improved data hiding in encrypted images, by Weiming Zhang, Kede Ma, Yu Elsevier 2014.
[3] Maniccam S.S., Bourbakis N.G., "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001) 1229-1245 Springer 2014
[4] Acharya B, Patra S. K., Panda G., "A Novel Cryptosystem Using Matrix Transformation", Proceedings of SPIT-IEEE Colloquium and International Conference, Mumbai, India, Vol. 4, 92 IEEE 2014.
[5] Gautam A, Panwar M, Gupta P. R., "A New Image Encryption Approach Using Block Based Transformation Algorithm", International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 8, Issue No. 1, 090 – 096 2013
[6] C. H. Kim, "Improved Differential Fault Analysis on AES Key Schedule", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 41-50, 2012.
[7] Zhang X, Feng G, Ren Y, and Qian Z. , "Scalable Coding of Encrypted Images", IEEE Transactions On Image Processing, Vol. 21, No.6, June 2012
[8] Zhang X, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE Transactions On Information Forensics And Security, Vol. 6, No. 1, March 2011
[9] Guo J M and Le T N, "Secret Communication Using JPEG Double Compression", IEEE Signal Processing Letters, Vol. 17, No. 10, October 2010
[10] Kushwaha J, Roy B., "Secure Image Data by Double encryption", International Journal of Computer Applications (0975 – 8887), Volume 5– No.10, August 2010
[11] Liu W, Zeng W, Dong L, and Yao Q, "Efficient Compression Of Encrypted Grayscale Images", IEEE Transactions on Image Processing, Vol. 19, No. 4, April 2010
[12] Yicong Z., Panetta K, Agaian S, Senior Member, "Image Encryption Using Binary Key- images" ,Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009

CITE AN ARTICLE

Khan, E., & Rai, D. (2018). IMAGE ENCRYPTION USING TRAPDOOR ONE WAY FUNCTION. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 7*(8), 592-598.