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:

\[ y_{img} = g(x); \text{is easy to calculate realltively} \]  \hspace{1cm} (i)

\[ x = g^{-1}(y_{img}) \text{is generally infeasible without additional information} \]  \hspace{1cm} (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:

\[ \frac{K_0}{2} (psd) = CONSTANT \]  \hspace{1cm} (iii)

Here,

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

CONSTANT is the value over the ranges of frequency
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:

\[ Z_1 \xrightarrow{T} L_1 \quad \text{(iv)} \]
\[ Z_2 \xrightarrow{T} L_2 \quad \text{(v)} \]
\[ \alpha Z_1 + \beta Z_2 \xrightarrow{\text{Trans}} L_1 + L_2 \quad \text{(vi)} \]

Here,

- \( Z_1 \) is input 1
- \( Z_2 \) is input 2
- \( L_1 \) is input 1
- \( L_2 \) is input 2
- \( \text{Trans} \) is transformation done by the system
- \( \alpha \) and \( \beta \) are system constants

The homogeneity principle states:

\[ Z_1 \xrightarrow{T} L_1 \quad \text{(vii)} \]
\[ a. Z_1 \xrightarrow{T} k. L_1 \quad \text{(viii)} \]

Here,

- \( a \) is a system constant

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

\[ G(x, y - Sht) \xrightarrow{H} X(x, y - Sht) \quad \text{(ix)} \]

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:

\[ PSNR = 10 \log_{10} \frac{\text{size}^2}{\sum_{i,j} (I - I')^2} \quad \text{(xi)} \]

Here,

- \( I \) is the x-pixels
- \( J \) is the y-pixels
- \( I \) is the image under interest
- \( I' \) represents image after process
\[ MSE = \frac{1}{ij} \sum_{i,j} (I - I')^2 \] (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)](lena.jpg)

![Fig.2 Test Image2 (cameraman.jpg)](cameraman.jpg)
Fig. 3 Encrypted Image using Proposed Methodology

Fig. 4 Image undergoing Blurring Effect
Fig. 5 Image undergoing Blurring and Gaussian Noise attack

Fig. 6 Image restoration with parameter NSR being zero
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.
REFERENCES


CITE AN ARTICLE