

# Image Encryption Techniques under Various Noise Attacks: A Survey

**Ms.Garima Pal**

M.Tech Scholar

LKCT, Indore (India)

**Prof.Vijay Verma**

Assistant Professor

LKCT, Indore (India)

**Abstract:** Encryption of data has been a major area of research for a long time. With the passage of time, the algorithms that have been used for text data have found applications in other data formats as well. With increasing advances in digital technology, digital images have started being used extensively for effective communication. Several image encryption algorithms have been tested for enhanced efficiency and throughput. Since images tend to undergo several degradations while capturing, storage and transmission, therefore several image restoration techniques have also been developed to circumvent the effect of various types of noise. This paper introduces the fundamentals of digital image processing and related aspects with focus on image encryption algorithms, image compression mechanisms and various types of noise affecting digital images.

**Keywords:** Image Processing, Image Encryption, Image Compression, Transform Domain, Chaotic Neural Network (CNN), Discrete Cosine Transform (DCT), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE).

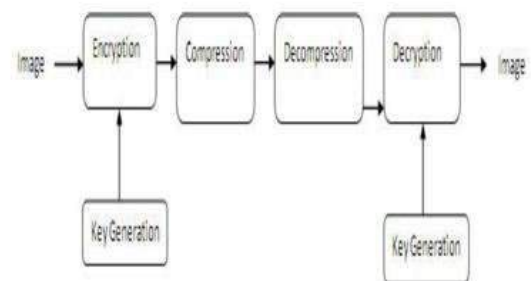
## 1. Introduction:

An image can be thought of as a two dimensional function,  $I = f(x, y)$  where  $x$  and  $y$  represent the coordinates of the picture elements or pixels.[1] Generally any image can be considered to be a large matrix of picture elements where the picture elements have two vital pieces of information associated with them:

- 1) The intensity of the picture elements or the gray scale value of the picture element.
- 2) The frequency information of the picture element or the R, G, B value associated with a point with fixed coordinates.

Generally digital images are processed using a digital computer in case of which the technique is called digital image processing (DIP). There are various changes which can be brought about in the digital images using digital image processing. Generally the manipulations are carried out in the gray scale value of the image, the R,G,B value of the image or the coordinates of the pixels of the image.

Image encryption is the technique of encrypting images by carrying out transformation in the pixel values of the image under consideration.



**Fig.1 Basic Encryption Model**

Image Encryption algorithms should satisfy the following conditions:

1. The algorithm should be applicable to a large spectrum of images viz. Photographic Images, Radar Images, Biomedical Images etc.
2. The algorithm should impart ample differences among the picture elements so as to ensure randomness in the image pixel regions.
3. Keys used in the image encryption algorithm should change dynamically so that the algorithm becomes more secure.

- The algorithm should not impart a high value of space or time complexity so as to facilitate practical utility.

## 2. Different Techniques used for Image Encryption:

**2.1 Random Pixel Exchanging Techniques:** In this technique, manipulations or transformations are carried out on the pixel values.[2] To impart randomness into the encryption algorithm, mathematical functions which show the highest amount of randomness and which are the most difficult to break by guessing attacks or brute force are used. Such mathematical operations are generally 'bitxor' operations or operations involving high order prime numbers. The fractional order of a gyrator transform may be used as an additional key for the algorithm. The concept can be understood with the help of the following system model:

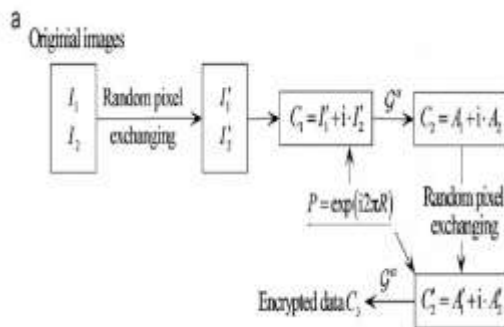


Fig.2 Model for Pixel Exchanging

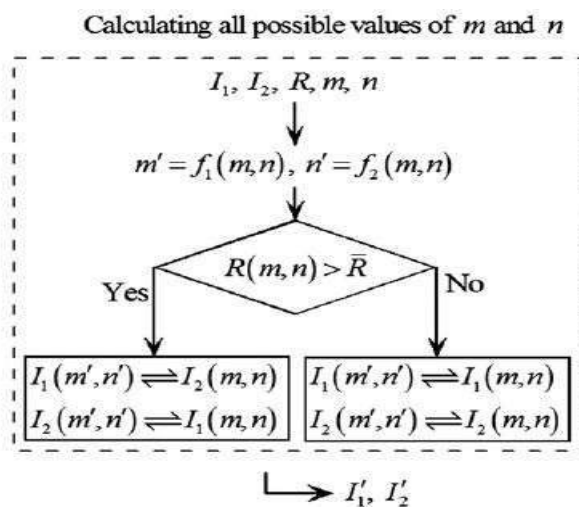


Fig.3 Random Pixel Exchange Techniques

The aforesaid technique can be mathematically explained as:

$$M' = f_1(m, n) \text{ and } N' = f_2(m, n),$$

Here the most important aspect is the design of the mathematical functions used for the encryption process. The mathematical functions have to be modelled in such a way that breaking them is infeasible over a period of time. The infeasibility can be computed in terms of the rate at which the algorithm grows and that of the computation complexity[1]. The following graph illustrates the fact.

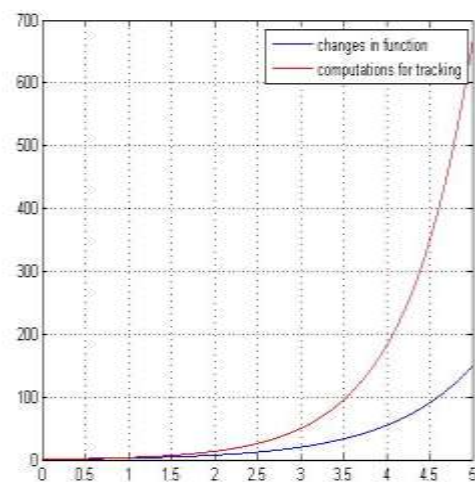


Fig.4 A measure of infeasibility in breaking an algorithm

It can be seen from the above graph that the computational complexity grows more rapidly compared to the growth of the algorithm. This imparts infeasibility to the algorithm.

## 2.2 Image Encryption in Transform Domain:

This encryption technique uses the transform domain approach for image encryption. The various types of transforms used under this category are the Fourier Transform, Fast Fourier Transform, Discrete Cosine Transform, Wavelet Transform, Contourlet transform. [7] Mathematically, it may be understood as:

$$I(m, n) \leftrightarrow I[d(m_d, n_d)]$$

Where  $(m_d, n_d)$  are the pixel values in the transform domain. After the manipulations are done in the transform domain, the image is brought back to the

original domain using the inverse counterpart of the transform. A basic description of the Transforms is given below:

### The Fast Fourier Transform (FFT) calculating the Fourier Transform Efficiently:

It is defined as”

$$X(k) = \sum_{j=1}^N x(j) \omega_N^{(j-1)(k-1)}$$

$$x(j) = (1/N) \sum_{k=1}^N X(k) \omega_N^{-(j-1)(k-1)}$$

where

$$\omega_N = e^{(-2\pi i)/N}$$

Where N is the number of pixel values.

### The Discrete Cosine Transform (DCT)

The DCT is a cosine counterpart of the Fourier Transform where the base function or the kernel of the transform is a cosine function. It has been observed that the Discrete Cosine Transform yields good results in the context of images. A mathematical definition of the Discrete Cosine Transform can be put forth as:

$$y(k) = w(k) \sum_{n=1}^N x(n) \cos\left(\frac{\pi(2n-1)(k-1)}{2N}\right) \quad k = 1, 2,$$

where

$$w(k) = \begin{cases} \frac{1}{\sqrt{N}} & k = 1 \\ \frac{2}{\sqrt{N}} & 2 \leq k \leq N \end{cases}$$

### The Wavelet Transform:

The wavelet transform is a relatively new form of the transforms compared to the Fourier Transform. This tool is basically used for the analysis of signals which do not follow the Dirichlet's conditions stated below:

- 1) The function should be absolutely integrable over a period.
- 2) The function must have finite number of discontinuities over a period.

- 3) The discontinuities should themselves be finite in nature.

Generally smooth signals which do not exhibit sudden changes follow these conditions. Images which are highly non-stationary in nature do not follow these conditions and hence are not suitable for analysis using the Fourier Transform. Hence a new tool with non-smooth or non-stationary base signals is introduced in the form of the Wavelet Transform.

Mathematically the *continuous wavelet transform* (CWT) can be defined as the sum over all time of the signal multiplied by scaled, shifted scaled, shifted versions of the wavelet function

$$C = \int_{-\infty}^{\infty} f(t) \phi\left(\frac{t-j}{k}\right) dt$$

(scale, position)

Where

1, 2...M-1, Here j is scaling factor and k is shifting factor for the transform.

The scaling function can be defined as:

Scaling function

$$W\Phi(j, k) = \frac{1}{\sqrt{M}} \sum_n S(n) \cdot \Phi(n)_{j, k}$$

The Wavelet Function can be defined as:

$$W\psi(j, k) = \frac{1}{\sqrt{M}} \sum_n S(n) \cdot \psi(n)_{j, k}$$

These are the basic transforms that are used for the encryption of images in the transform domain.

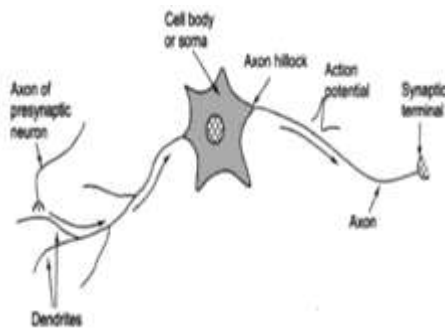
### 2.3 Encryption using Neural Network:

Neural networks tend to utilize that fact that the human brain works and processes data in a manner very different from even the most advanced digital computers. The human brain exhibits the following important traits:

- 1) A High level of non-linearity
- 2) A highly parallel paradigm or structure.

It is due to these traits that the human brain can accomplish enormous tasks within fractions of seconds which is takes enormous amount of time for even the most powerful computing platforms.

The basic biological model of a neuron is shown below.

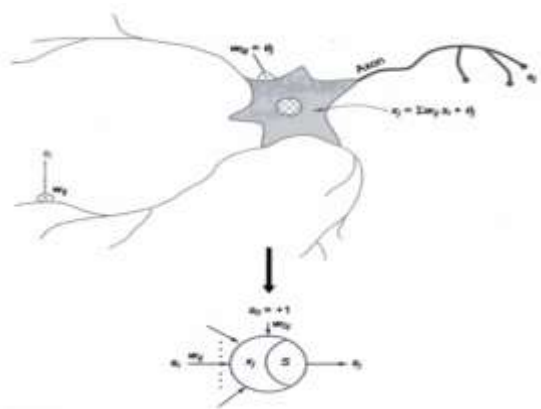


**Fig.5 Biological model of neuron**

Analysis of the biological model points towards the parallel structure of the human brain where signals from different parts of the human body accumulate simultaneously at the brain. The mathematical equivalent of such a model can be given by:

$$\sum_{i=1}^n X_i W_i + \Theta$$

here  $X_i$  represents the signals coming from different paths,  $W_i$  represents the weight corresponding to a particular path and  $\Theta$  is the bias of the network. The aforesaid can be understood as:



**Fig.6 Mathematical model of a neural network**

### Encryption using Chaotic Neural Network

Image encryption using chaotic neural networks is a rather evolving area of research. The roots of this technique stem from the proposition of chaos theory by Robert May. Chaos can be understood as a condition in which the output of the system is fixed for a particular input but changes in the input yield a completely different output thereby not following any fixed mapping between input and out parameters of the system. Thus the system changes

its structure according to the variations in the inputs that it receives.[4]

The above condition can be understood as:

$$Y(i) = f(X(i)) \quad \forall X(i);$$

But  $Y(i)$  is random for  $X(i+\Delta)$ ;

where  $\Delta$  stands for a change in  $X$ .

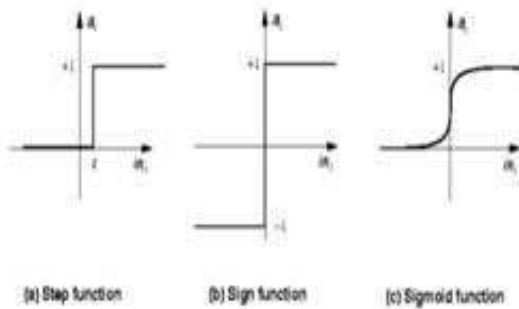
The above mathematical conditions can be utilized to create what is called a 'chaotic neural network' i.e. a neural network exhibiting the property of chaos. [3], [5] The existence of chaos in the neural network implies that the structure of the network varies or changes dynamically with the variations in the received input of the network. The mentioned condition can be mathematically designed as:

$$W(i) = f'(X(i));$$

here  $f'$  depicts the function responsible for changing the weights and structure of the network continuously. As the weights of the different paths keep changing dynamically, hence the structure of the neural network also keeps changing dynamically. Thus even if the attackers coincidentally come to predict the nature of the neural network at a given time 't', still continuous change would make it of no avail.

The various activation functions that are used in the design of chaotic neural networks are shown below:[5]

## Activation Functions



- $\text{Step}_t(x) = 1$  if  $x \geq t$ , else 0 threshold= $t$
- $\text{Sign}(x) = +1$  if  $x \geq 0$ , else  $-1$
- $\text{Sigmoid}(x) = 1/(1+e^{-x})$

**Fig.7 Different Activation Functions**

The activation functions in general decide the type of decision the neural network takes when subject to different conditions due to the continuously changing values of the input under consideration. While some activation functions depict a sudden or step change in the decision, others exhibit a gradual change in the decision output corresponding to the changing input values.

### 2.4 Encryption utilizing Map-Lattice Technique

In the proposed method, an image encryption scheme which uses the spatiotemporal dynamics of the mixed linear–nonlinear coupled map lattices system is used.[8], [9]. The mixed non linearity of the map lattices results in the high amount of randomness of the ciphers generated and thus imparts a high level of security in the employed system. The key length is kept to be more than 400 bits which generates the initial conditions of the maps used for encryption. The technique utilizes the property of chaos similar to the concept of the chaotic neural networks with the exception that the structure of the map lattices change dynamically with the dynamics of the map lattices. The bit level exchange helps to accomplish non redundancy in the image pixel values thereby improving the quality of the image. What it also does is that it removes any linear traits in the pixel values which may be utilized by attackers to break the algorithm. The sensitivity of the map lattice parameters clearly

suggest that the algorithm becomes infeasible to break by brute force or guessing attacks. The comparative analysis of the algorithms suggests that it achieves higher level of security and randomness compared to several other algorithms. Mathematically its defined as:

$$X_{(n+1)}(i) = (1-\epsilon)f[x(i)] + [\epsilon/2]\{X_{(n+1)}(i) + X_{(n-1)}(i)\}$$

Here,  $\epsilon$  is the coupling parameter and  $f$  is the mapping function

### 2.5 Encryption utilizing Pixel Diffusion Process

In the hash based multiple diffusion process, a 512-bit long external secret key is used as the input value of the salsa 20 hash function. The key space is large enough to resist brute-force attacks. The key stream in the encryption process depends on both the initial keys and the plain-image. [9], [10] The proposed method is a private key encryption system with only two rounds of diffusion process. The diffusion process is such that the pixel correlation is minimalistic thereby rendering difference in nature to the picture components of the image of interest. Lower value of pixel similarity doesn't allow adversaries to pick up patterns in the encrypted image. This results in high level of security yet comparatively less computational complexity.

## 3. TYPES OF NOISE

Digital images undergo various transformations during storage in memory devices, capturing using capturing devices, transmission through various wired and wireless channels and retrieval through various receivers. The unwanted signals or degradations affecting digital images are termed as noise.

Image noise can be classified as

- Gaussian Noise (Amplifier Noise)
- Poisson Noise (Shot Noise)
- Salt & pepper Noise (Impulse Noise)
- Spackle Noise

### 3.1 Gaussian Noise (Amplifier Noise)

Gaussian noise which is also known as electronic noise or amplifier noise because it primarily arises out of the amplifiers designed in the devices of various stages of image capturing, storage, transmission and retrieval. This type of noise is independent of the gray scale value or intensity of pixels occupying different coordinates. It has a flat power spectral density, i.e. it is independent of the spectrum that the image occupies. Ideally it is a zero mean noise with the standard deviation or variance indicating the amount of deviation of the noise value from the mean value. The most challenging part in removal of this noise is that it occupies an ultra wide spectrum thereby making the filtering process very difficult.

### 3.2 Salt & pepper Noise (Impulse Noise)

Salt and pepper noise is sometimes called impulse noise or spike noise due to its impulsive nature to affect only in certain frequency bands. A typical appearance of this type of noise is black and white spots resembling the appearance of salt and pepper granules. The noise has only two discrete values or levels corresponding to which the salt and pepper appearance take place. [12].

This kind of a noise can result from the non linear quantization process of quantizers, errors in analog to digital converters or digital to analog converters. It can also arise out of the errors in the sensors installed for capturing the image pixel values.

## 4. Performance Indices:

The Peak Signal to Noise Ratio (PSNR) and mean square error (MSE) serve as two vital parameters in deciding the effect of degradations in the image. While MSE is a measure of the errors in the image with respect to the original image, PSNR indicated the effect of residual noise. [14].

### Mean Square Error (MSE)

The MSE represents the cumulative squared error of the original image and the image has undergone some transformation. The accuracy of any algorithm can be decided based on this metric that computes the mean difference between the original image and the distorted image.

### 3.3 Speckle Noise (Multiplicative Noise)

Speckle noise follows a multiplicative pattern and the effective pixel value is the original pixel value plus the noise coefficient multiplied with the original pixel value.

$$J = I + n * I$$

here, J is the noise distribution of speckle noise, I is the original image under consideration. The speckle noise is a result of the non impulse response of the transmission media through which the images propagate. The convolution in the time domain results in multiplication in the transform domain thereby making the noise appear multiplicative in nature.

### 3.4 Poisson Noise (Shot Noise)

Poisson or shot photon noise arises due to the fact that the image sensors may not always be able to capture the number of pixels needed for the true representation of the image. In such cases the sensor or reproducing system adds pixels of its own to recreate the image. The degradations occur since the extra added pixels are not a derivative of the original image. It can also arise of the random motion of charge carriers in the devices or equipments which the image passes through. Since heating up of equipments causes random motion of charge carriers, hence this kind of noise is encountered.

$$MSE = \frac{1}{MN} \sum_{X=1}^M \sum_{Y=1}^N (F(X,Y) - I(X,Y))^2$$

A low value of MSE indicates lower degradation occurring to the original image, while a higher value indicates higher degradations.

### Peak Signal Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) indicates the amount of residual noise present in the image under consideration. The higher the value of signal power and the lower the value of the image power, higher is the value of PSNR. Peak Signal to Noise Ratio is usually expressed in decibels since it is a ratio of powers. It is mathematically expressed as:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \text{ dB}$$

A high value of PSNR indicates that residual noise is still present in the image and needs to be removed by some filtering techniques.

### Relation between MSE and PSNR

The values of MSE and PSNR follow a specific pattern which seems to be correlated. The correlation stems from the fact that the degradation or noise effects in the image turn out to be manifested at the pixel level and higher degradation imply higher values of MSE. The mean value of the errors of two images correspond to the changes in the two images that may have taken place due to unwanted transformation of the pixel coordinates, or the pixel intensity often defined by the gray scale value or the GRB value of the pixel which are a measure of the frequency spectrum occupied by the image.

PSNR on the other hand is inversely proportional to the MSE value since the degradation occurring in the image which is manifested in the form of MSE because the noise effects to creep into the image. Thus higher values of MSE tend to bring down the value of PSNR. It is customary for systems to increase the MSE and hence lower the values of PSNR in which images undergo pixel changes. A simultaneous plot of MSE and PSNR helps in understanding the effects of degradations on the images. Several filtering and restoration techniques are utilized to invert the process or rather the degradation process of the systems that the images encounter. A mathematical modelling of such degradations is necessary at the outset for designing an inverting process. The technique of removing noise and restoring the original image with priori information is called image restoration.

**Table.1 Comparison of different encryption algorithms**

S.No	Technique	Advantage	Disadvantage
1	Random Pixel Exchanging Techniques:	Bit-wise operations needed, hence low complexity yet high level of security	Difficult to design multiple functions exhibiting low pixel correspondence
2	Image Encryption in Transform Domain	Difficult to decipher due to changes in transform domain	Image degradation due to transform and inverse transform
3	Encryption using Chaotic Neural Network	Immune towards decryption due to presence of 'chaos'	Extremely difficult to model a chaotic system
4	Encryption using Map-Lattices	Immune to attacks due to many to one multiple correspondence functions	Enhanced complexity thereby reducing system throughput

5	Encryption using Pixel Diffusion Process	Difficult to find exact locations of randomly injected pixels by adversaries	System throughput suffers due to overhead addition of pixels
---	--	--	--

IJournals

**Conclusion:** It can be concluded that the digital images can be encrypted using various algorithm which have their own merits and demerits. The important parameters of an image encryption algorithm are randomness, space and time complexity. While complex mathematical formulations may make attacks infeasible, it may render infeasibility to the practical implementation of the designed system. Another important feature is the effect of noise or degradations of the image which need to be negated using proper denoising or restoration techniques. Finally the effectiveness of any algorithm can be measured in terms of MSE and PSNR.

### References

- [1] Reversibility improved data hiding in encrypted Images, Weiming Zhang, Kede Ma, Nenghai Yu, Elsevier, 2013
- [2] Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains, Elsevier 2012, Zhengjun Liu , Yu Zhang , She Li , Wei Liu , Wanyu Liu , Yanhua Wang, Shutian Liu
- [3] Color image encryption using spatial bit-level permutation and high-dimension Chaotic system, Elsevier 2011 Hongjun Liu , Xingyuan Wang
- [4] NPCR and UACI Randomness Tests for Image Encryption Yue Wu, Student Member, IEEE, Joseph P. Noonan, Life Member, IEEE, and Sos Aгаian, Senior Member, IEEE 2011
- [5] A novel colour image encryption algorithm based on chaos, Elsevier 2011 Xingyuan Wang, Lin Teng, Xue Qin
- [6] A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Elsevier 2011 Seyed Mohammad Seyedzadeh n, Sattar Mirzakuchaki
- [7] Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding, Elsevier 2012 Zhengjun Liu, She Li, Wei Liu, Yanhua Wang, Shutian Liu
- [8] A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice, Elsevier 2014 Zhang Ying-Qian, Wang Xing-Yuan
- [9] A novel image encryption based on hash function with only two-round diffusion process, Springer 2013 Benyamin Norouzi, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, Mohammad Reza Mosavi
- [10] A novel chaotic block image encryption algorithm based on dynamic random growth technique, Elsevier 2014 Xingyuan Wang, Lintao Liu, Yingqian Zhang
- [11] Lag Synchronization of Switched Neural Networks via Neural Activation Function and Applications in Image Encryption, IEEE Transactions 2014 Shiping Wen, Zhigang Zeng, *Senior Member, IEEE*, Tingwen Huang, *Senior Member, IEEE*, Qinggang Meng, and Wei Yao
- [12] A Comparative Study of Various Types of Image Noise and Efficient Noise Removal Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, IJRCSSSE 2013 Rohit Verma, Jahid Ali
- [13] Comparative Study of Different Noise Models and Effective Filtering Techniques, International Journal of Science and Research (IJSR) Dr. Aziz Makandar, Daneshwari Mulimani, Mahantesh Jevoor
- [14] Efficient Technique for Colour Image Noise Reduction C.Mythili, V.Kavitha The Research Bulletin of Jordan, ISWSA; ACM 201