**International Journal of Contemporary Technology and Management**
Volume VI, Issue IV, May - 2017 ISSN (Online) 2278-8034

# A Survey and Taxonomy on Image Encryption Techniques

Aman Verma
M.Tech Scholar (ECE)
SDBCT, Indore
amanverma142@gmail.com

Vinod Sonkar
Asst.Professor (ECE)
SDBCT, Indore
vinodk.sonkar@gmail.com

Deepak Sharma
Asst.Professor (ECE)
SDBCT, Indore
er_deepak07@yahoo.co.in

**Abstract:** With the advent of digital technology, digital images have gained unprecedented importance. Digital images are being used in medicine, telecommunications, defence etc. Therefore a need of securing the images from unauthorized users and adversaries has emerged as a serious challenge. The single most important technique used for image security has been image encryption. Several image encryption techniques have been investigated but each has its own pros and cons.[1],[3] While capturing, storage and transmission, images undergo several degradations due to noise and blurring effects. Also, images being large in size pose a challenge in storage and transmission. This paper explains the empirical image encryption techniques along with the sources of noise and degradations. Finally image compression techniques have been discussed.

**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 may be defined as a two dimensional function, I= *f(x, y)* where x and y are spatial co-ordinates i.e. co-ordinates corresponding to space or location.[1] The function I essentially contains two basic pieces of information, one being the intensity at a point also called the gray scale value and the R-G-B value which tells about the colour or frequency aspect of the image. If it happens so that the values of (x, y), and the gray level [*f(x, y)*] are finite and discrete values, then such an image is called a digital image.

If we process the digital images using a digital computer, then this process is called digital image processing. Digital images comprise of finite number of elements each of which has a finite location and value. These elements are called picture elements, image elements, or pixels. Digital images have immense applications ranging from education, defence and military, banking, electronic vision, photography to video filming, medical etc. But during the capturing, storage and retrieval, transmission and receiving of images, they are affected by various types of noise. This process degrades the quality of the images and the degradation can be nominal to severe depending upon the degradation phenomena.

Image encryption can be understood using the following model:

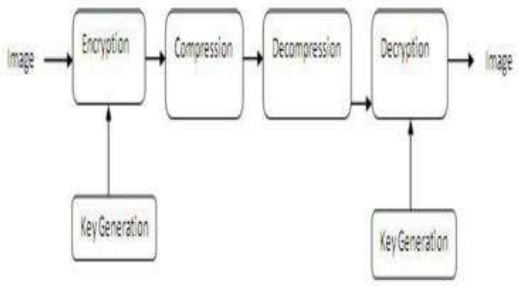


**Fig.1 Basic Encryption Model**

Any encryption model should satisfy the following conditions:

1. It should be able to secure various types of images viz. Photographic Images, Radar Images, Biomedical Images etc.
2. It should render a high amount of randomness to the encrypted data making it infeasible for the adversaries to decrypt by brute force.
3. The key used in the algorithm should change with the state of the images so as to ensure higher levels of security.
4. Finally, it should not be too complex to implement on hardware.

## 2. Various Techniques for Image Encryption:

**2.1Random Pixel Exchanging Techniques:** In such techniques, random pixel exchanging and random phase encoding in gyrator domains is designed. Two original images are regarded as the real part and imaginary part of complex function during the starting stage of encryption process.[1].Subsequently, the complex function is encrypted by the two operations mentioned above.

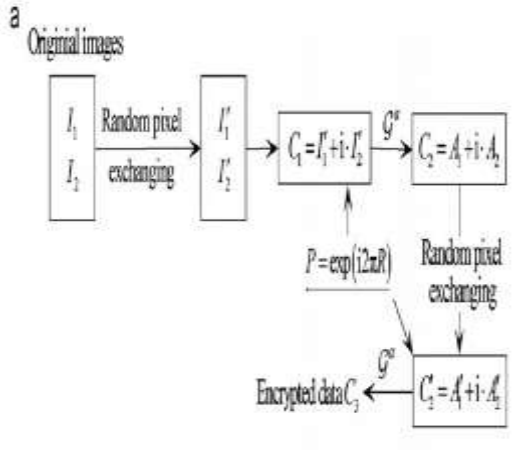


**Fig.2 Model for Pixel Exchanging**

A random matrix R is employed in both pixel exchanging and phase coding for reducing the space storing keys in the application of storage and transmission of secret information.[2] The fractional order of a of gyrator transform can serve as an extra key. The concept can be understood with the help of the following system model:

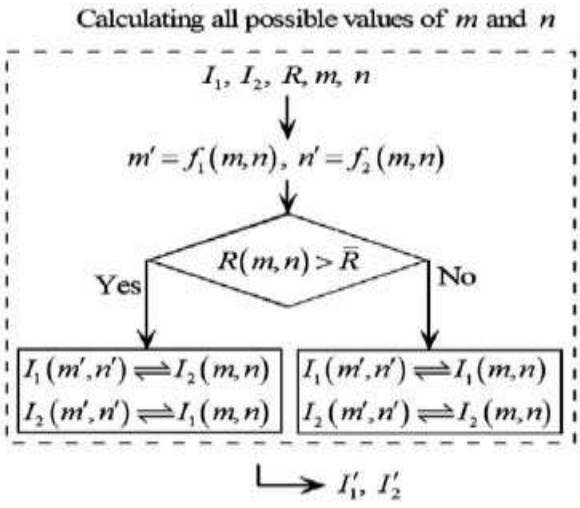


**Fig.3 Random Pixel Exchange Techniques**

The random pixel exchanging algorithm cab be mathematically defined as:

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

where m and n are the pixel values and $f_1$ and $f_2$ are the random functions deciding the new encrypted pixel values form the original ones. The main challenge of such techniques is the design of a strong function $f_1$ and $f_2$ whose inverse would be computationally infeasible to compute.

**2.2Image Encryption in Transform Domain:** In this category of encryption techniques, the image is first converted to the transform domain using some mathematical transform such as the Fourier Transform, Fast Fourier Transform, Discrete Cosine Transform, Wavelet Transform, Contourlet transform. [7] Mathematically, it can be defined as:

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

Where $\mathbf{(m_d,n_d)}$ are the pixel values in the transform domain. The image is again brought

back in the original domain using the inverse 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 defined as:

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

where

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

**The Wavelet Transform:**

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

$$C\ (scale,\ position) = \int_{-\infty}^{\infty} f(t)\ ((scale, position, t)\ dt$$

Where

1, 2…M-1, Where j is scaling factor and k is shifting factor

Scaling function

$$W\Phi\ (Jo, k) = \frac{1}{\sqrt{M}}\sum_n S(n).\Phi(n)_{jo'k}$$

Wavelet Function

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

Several other transform domains can be used depending upon the type of application.

**2.3Encryption using Neural Network:**

Work on artificial neural network has been motivated right from its inception by the recognition that the human brain computes in an entirely different way from the conventional digital computer.[5],[11] The brain is a highly complex, nonlinear and parallel information processing system. It has the capability to organize its structural constituents, known as neurons, so as to perform certain computations many times faster than the fastest digital computer in existence today. The brain routinely accomplishes perceptual recognition tasks, e.g. recognizing a familiar face embedded in an unfamiliar scene, in approximately 100-200 ms, whereas tasks of much lesser complexity may take days on a conventional computer. A neural network is a machine that is designed to model the way in which the brain performs a particular task. The network is implemented by using electronic components or is simulated in software on a digital computer. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for use. It resembles the brain in two respects,[11]

1. Knowledge is acquired by the network from its environment through a learning process.

2. Interneuron connection strengths, known as synaptic weights, are used to store the acquired knowledge.

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. Other advantages include:

1. Adaptive learning**:** An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organization**:** An ANN can create its own organization or representation of the information it receives during learning time.
3. Real Time Operation**:** ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.

The biological model of the neuron is shown in the figure. It consists of the cell body, axon hillock, action potential, synaptic terminal, axon of pre synaptic neuron and dendrites. Signals from different parts of the body travel through different parts and reach the neuron where the neuron processes it and produces an output.

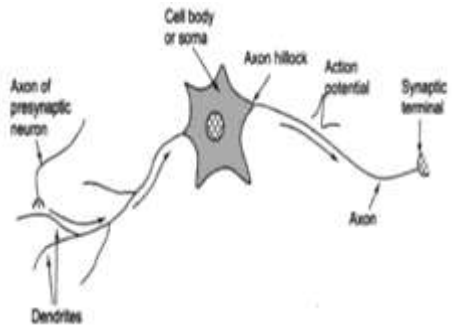


**Fig.4 Biological model of neuron**

It should be noted though that the output of a neuron may also be fed to another neuron. A collection of such neurons is called a neural network. The neural network can perform simple to complex tasks depending on the structure of the neural network.

After studying the basic biological model of the neural network, a mathematical model is envisaged to be designated. The mathematical model for such a neural network is given by:

$$\sum_{i=1}^{n} XiWi + \theta$$

Where Xi represents the signals arriving through various paths, Wi represents the weight corresponding to the various paths and Θ is the bias. The above concept can be visualized by the following diagram:

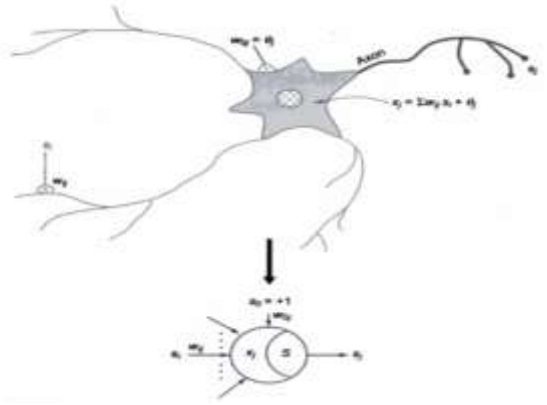

**Fig.5 Mathematical model of a neural network**

The above diagram exhibits the derived mathematical model of the neural network. It can be seen that various signals traverssing different paths have been assigned names X and each path has been assigned a weight W. The signal traverssing a particular path gets multiplied by a corresponding weight W and finally the overall summation of the signals multiplied by the corresponding path weights reaches the neuron which reacts to it according to the bias Θ.

**Encryption using Chaotic Neural Network**

Encryption using an artificial neural network is a relatively new field of research.[10]. The reason behind employing neural networks for encryption is the highly **parallel and non-linear** nature of the human brain. The aforesaid characteristics of the human brain are tried to be replicated using an artificial neural network. The main aim in designing such a network is the presence of **'chaos'.**

Chaos refers to the following condition:

If the output of a system is deterministic for a particular input, but the output cannot be predicted if the input is changed from its present state leads to the existence of chaos in the system.[4] Mathematically, the above condition can be expressed as:

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

But Y (i) is random for X (i+Δ);

where Δ stands for a change in X.

Such a mathematical condition can be generated by what is called a **'chaotic neural network'** i.e. a neural network that exhibits the property of chaos. [3], [5] Chaos is the property that makes it extremely complicated for the attackers to break the encryption algorithm and decipher the cipher text. The requirement for such a chaotic neural network is the adaptive nature of the path weights for different conditions. As the path weight variable changes adaptively, the design of the neural network changes for various inputs thus making it infeasible for the attacker to decipher the cipher text. The above condition can be mathematically expressed as:

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

where f ' represents the function or condition that keeps changing the path weight according to the input available to the chaotic network.

Since the path weights change according to the available inputs, therefore the encryption taking place through the chaotic neural network keeps changing dynamically.

The different activation functions that can be used for deciding the output of the neural network are given below:[5]

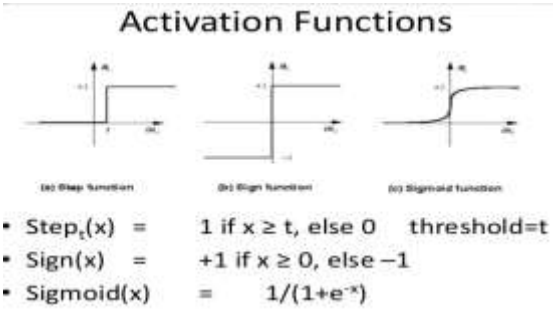


**Fig.6 Didderent Activation Functions**

The above figure describes the common activation functions generally used in chaotic neural networks. Since we need to use hard thresholding or gardlimiting function in our proposed work, therefore we use the step function which decides about a threshold 't'.

The main motive behing using chaotic neural nwtworks (CNN) is the randomness it imparts to the encrypted pixel values.

**2.4Encryption using Map-Lattices**

In the proposed method, an image encryption scheme which uses the spatiotemporal dynamics of the mixed linear–nonlinear coupled map lattices system.[8], [9] Due to the given new features in dynamics of the mixed linear–nonlinear coupled map lattices system, the coupling structures have enhanced the cryptosystem security. A more than 400 bit-long secret key has been used to generate the initial conditions and parameters of the maps. The encryption policy is crucial to a chaos-based cryptosystem as well as choosing a suitable chaotic system. The proposed algorithm also employs a new bit-level permutation which is able to reduce the intrinsic redundancy of an image and save space storage in the execution. The security

analyses are given to prove that the key space and sensitivity is better enough to make brute-force attacks infeasible. Simulations have been carried out to compare its performance with the former encryption algorithms. The results show that the proposed algorithm leads to a higher security level compared to previous techniques. These results justify the superior security of the proposed cryptosystem. Mathematically its defined as:

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

Here, ε is the coupling parameter and f is the mapping function

**2.5Encryption using 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 are prone to a variety of types of noise. Noise is the undesirable effects produced in the image. [12], [13]. During image acquisition or transmission, several factors are responsible for introducing noise in the image. Noise may be modelled by either the Histogram or probability density function. Noise is superimposed on original images.

Depending on the type of disturbance, the noise can affect the image to different extent. Generally our focus is to remove certain kind of noise. So we identify certain kind of noise and apply different algorithms to remove the 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)**

It is also called as electronic noise or amplifier noise because it arises in amplifiers or detectors. This noise model is additive in nature [12] and follow Gaussian distribution. Meaning that each pixel in the noisy image is the sum of the true pixel value and a random Gaussian distributed noise value. The noise is independent of intensity of pixel value at each point. Gaussian noise generally disturbs the gray values in digital images.

Gaussian noise caused by natural sources such as thermal vibration of atom, discrete nature of radiation of warm objects and conversion of the optical signal into an electrical one. Gaussian noise can be reduced using a spatial filter.

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

Salt and pepper noise is sometimes called impulse noise or spike noise or random noise or independent noise or data drop-out noise. Black and white dots appear in the image [12] as a result of this noise and hence salt and pepper noise.

In Salt and pepper noise model has only two possible values, *a* and *b*. The probability of each is typically less than 0.1(otherwise, the noise would vastly dominate the image). The

corrupted pixels are set alternatively to the minimum or to the maximum value, giving the image a "salt and pepper" like appearance. Unaffected pixels remain unchanged. For an 8-bit/pixel image, the typical value for pepper noise is close 0 and for salt noise is close to 255. An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions [13]. This type of noise can be caused by dead pixels, analog-to digital converter errors and bit errors in data transmission, malfunctioning of pixel elements in the camera sensors, faulty memory locations, or timing errors in the digitization process.

**3.3 Speckle Noise (Multiplicative Noise)**

Speckle noise is a multiplicative noise .This noise can be modelled by random value multiplications with pixel values of the image and can be expressed as

J = I + n*I

Where, J is the speckle noise distribution image, I is the input image and *n* is the uniform noise image by mean *o* and variance *v*.

While Gaussian noise can be modelled by random values added to an image, speckle noise can be modelled by random values multiplied by pixel values hence it is also called multiplicative noise. Speckle noise is a major problem in some radar applications. Speckle noise follows a gamma distribution.

**3.4 Poisson Noise (Shot Noise)**

Poisson or shot photon noise is the noise that can cause, when number of photons sensed by the sensor is not sufficient to provide detectable statistical information [13]. This noise has root mean square value proportional to square root intensity of the image. Different pixels are suffered by independent noise values. At practical grounds the photon noise and other sensor based noise corrupt the signal at different proportions. Shot noise follows a Poisson distribution, which is usually not very different from Gaussian.

## 4. Performance Indices:

The Peak Signal to Noise Ratio (PSNR) and mean square error (MSE) are the two important performance parameters which are used to measure the quality of image [14].

**Mean Square Error (MSE)**
The MSE represents the cumulative squared error between the encoded and the original image. The effectiveness of the algorithm stands in minimizing the mean square error. If F(X, Y) is the original image, G(X, Y) is the corrupted image and I(X, Y) is the denoised image then MSE is given by

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

A low of MSE indicates that the original and the denoised image are close in characteristics. The reason being the fact that the MSE

**Peak Signal Noise Ratio (PSNR)**

PSNR represents a measure of the ratio between maximum powers of signal to the power of noise. We are trying to increasing the value of PSNR to the extent possible. PSNR is inversely proportional to the MSE; its unit is in decibel (dB) and is formally defined by the following equation.

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

A high value of PSNR indicates that the effect of noise has been mitigated.

It should be noted that that the lesser the value of MSE, the higher will be the value of PSNR. It can be understood from the fact that the differences in the pixel values occur due to the unwanted effects of random signal interferences such as noise.

**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 |

**Conclusion:** It can be concluded that different image encryption techniques can yield different types of encryption performance. The complexity of the different encryption techniques can be compared on the basis of encryption evaluation parameters such as CPU time and throughput. An important aspect of any image encryption algorithm is the mean square error and the throughput. Pixels undergoing encryption, noise effects and decryption cannot be completely restored. The amount of deviation of the decrypted image from the actual image or original image is measured using the Mean Square Error. The less the value of this error, the better is the performance of the encryption algorithm. The effect of noise on the image is evaluated using the Peak Signal to Noise Ratio. A high value of PSNR indicates lesser residual effect of noise.

**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 Agaian, Senior Member, IEEE 2011
[5] A novel colour image encryption algorithm based on chaos, Elsevier 2011 Xingyuan Wangn, 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, IJRCSSE 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