A Comprehensive Survey on Image Encryption Employing Chaos and Transofrm Domain Data Embedding

Tukaram Solanki[1] Prof. Sanmati Jain[2]

***Abstract*— Data Encryption has been one of the pivotal domains for research. For a long time is has happened to be a field of enormous research work because of its aspect of strong data protection. Initially data used to be handled in text formats only, but with time and advancement, data became available in various other formats as well other than just text. With progress in technology, the advent of digital images also started becoming rampant on a rapid scale. They are implemented in diverse systems of communication. Encryption concept also started getting prominence as a part of safeguarding method. A number of encryption algorithms have been put forth and have been tested with respect to their robustness and efficacy. Image degradation due to continuous capture and transmission has also been looked upon, in order to minimize the noise impact. This paper outlines the basics of digital image processing and allied concepts with its principle highlight on image encryption methods and the different kinds of noise laying impact on the 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).

I. INTRODUCTION

We can think of image to be of two dimensions, given by the two dimensional function I= *f(x, y)*: where co ordinates are given by x and y, which are also termed as pixel values. An image is a kind of a huge picture element matrix consisting of two major pieces of data related to them as follows[1]-[2]:-

1) The gray scale value of the picture element also called the intensity of the image.

2) The R, G, B value pertinent to points with fixed coordinates.

Digital images in general make use of a digital computer for data processing. This method is called Digital Image processing [3]. The digital images are processed in a digital manner by it. Many changes and modifications can be brought upon by the use of that method. The variations are mainly used in the gray scale value of the picture among the R,G,B values of the image pixels[4].

Image encryption of images is a mechanism of encryption where the pixels values of the images are transmogrified.

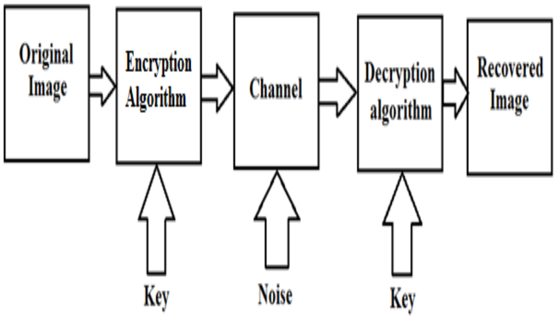

Fig.1 Basic Encryption Model

Following conditions need to be fulfilled in case of image encryption [5]:

1. A huger range of images must be able to be catered by the algorithm of encryption [6].

2. There must be a good amount of variations that the algorithm is able to introduce to achieve randomness of the regions of image pixels[7].

The robust keys must be employed such that the keys show dynamic changes to ensure greater security of the algorithm [8].

The algorithm must be feasible and practically implementable imparting less complexity in both time and space[9].

II. VARIOUS TECHNIQUES FOR IMAGE ENCRYPTION

A. *Random Pixel Exchanging Techniques:*

In this method, the image pixel values are changes or transformed. For greater randomness into the encryption method, the math functions that exhibit greater measure of randomness are utilized accordingly[10]. These tend to be the most hard to be breached by brute force attacks. Those mathematical functions with strong randomness quotient happen to be the '**bitxor'** operations that entail use of a greater number of prime numbers [11]. Gyrator transform with fractional order can also be utilized in addition to that. Following figures give lucid illustration of the concepts involved [12]:-

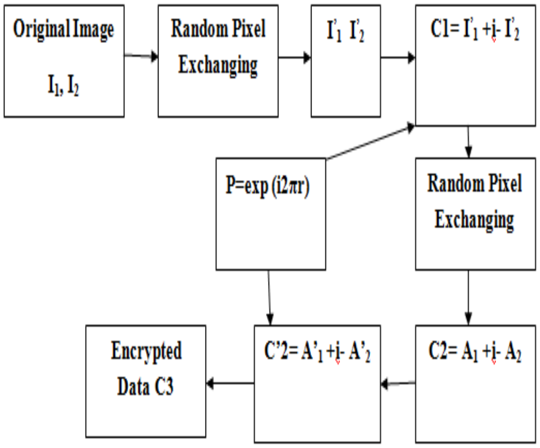

Fig.2 Model for Pixel Exchanging

This above method can be mathematically expressed as:

$M^{'}=g_1(m,n)=$ and $N^{'}=g_2(m,n)$,

Here g1 and g2 represent the transform functions and M' and N; the pixel coordinates [13].

The necessary consideration is the overall robust design of the math functions utilized for the encrypting method [14]. These functions must be robust enough such that it becomes nearly impossible to attack and breach them over a span of time domain. The attacks must become infeasible after a certain period of time. The infeasibility can be calculated with respect to the rate of growth of the algorithm and the computation complexity[15].

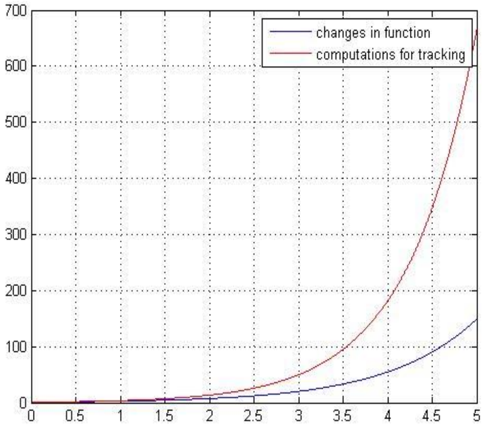

Fig.3 A measure of infeasibility in breaking an algorithm

Clear observation can be drawn from the above figure of graph suggesting the complexity of computation grows very fast in comparison to the algorithm growth rate.[16] This is an indication of provision of infeasibility to the encryption algorithm [17]

B. *Image Encryption in Transform Domain*

Here various transform domain approaches are utilized. [18].The types of transforms implemented pertinent to this category are the Fourier Transform, Fast Fourier Transform, Discrete Cosine Transform, Wavelet

Transform, Contourlet transform. Its expression in mathematics can be stated as [19]:

$I(m,n) \leftrightarrow I[d(m_d,n_d)]$ (1)

Where **(m_d,n_d)** denote the pixel values in the transform domain. The image is changed back into the original form domain using the inverse form of the transform after introducing required changes in the transform domain. A brief generic explanation of the concept is outlined as follows [2]:

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

It is defined as"

$$X(k) = \sum_{j=1}^{N} x(j)\omega_N^{(j-1)(k-1)} \quad (2)$$

And

$$x(j) = \frac{1}{N}\sum_{k=1}^{N} X(k)\omega_N^{-(j-1)(k-1)} \quad (3)$$

Here N is the number of pixel values.

The Discrete Cosine Transform (DCT)

DCT happens to be the cosine alternative of the Fourier Transform .In this the base function of the transform is a cosine function [21]. It has been marked that the use of DCT with respect to images, happens to give efficient results and improved performance. Discrete Cosine Transform in mathematical terms is outlined as below [22]:-

$$y(k) = w(k)\sum_{n=1}^{N} x(n) cos\frac{\pi(2n-1)(k-1)}{2N} \quad (3)$$

k=1,2......N

where,

$w(k) = \frac{1}{\sqrt{N}}$; for k=1

$w(k) = \sqrt{\frac{2}{N}}$; for 2<k<N

The Wavelet Transform:

This kind of transform is a relatively a newer version compared to all the existing Fourier transforms. This transform is generally implemented for the signal analysis where signals don't follow the Dirichlet's conditions stated below [23]-[24]:

1) The function is 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 [25].

Basically the signals that are smooth in nature and don't exhibit abrupt changes and variations adhere to these conditions. Images which show high fluctuating nature in terms of variations don't suit to these conditions and are therefore infeasible to be analysed by using Fourier Transforms. Hence the Wavelet Transform is introduced as a more unstable tool that can handle abrupt varying signals and non stationary base signals [26]..

The mathematical expression of the *continuous wavelet transform* (CWT) can be stated as the sum over complete time of the signal multiplied by scaled, shifted scaled, shifted versions of the wavelet function

$$C\ (scale,\ position) = \int_{-\infty}^{\infty} f(\mathrm{t})\ ((scale, position, t)\ dt \quad (4)$$

Where

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

The scaling function is given mathematically as:-

Scaling function

$$W\Phi\ (\mathrm{Jo,\ k}) = \frac{1}{\sqrt{M}}\sum_n S(n).\Phi(n)_{jo,k} \quad (5)$$

The Wavelet Function can be defined as:

$$W\psi\ (\mathrm{j,\ k}) = \frac{1}{\sqrt{M}}\sum_n S(n).\psi(n)_{j,k} \quad (6)$$

The aforementioned functions form to be the generic transform methods employed for image encryption in the transform domain [27].

C. Encryption using Neural Network:

Neural networks work on the basis of the fact that our human brain works in a vastly different manner and process the information the most unique ways compared to the top high end digital computers. The human possesses the below mentioned characteristics:

1) Great measure of non-linearity

2) An enormously parallel structure.

This is the reason why the human brain can compute and achieve huge works and processing of complex data in a matter of fractions of time that the most advanced computer takes great amount of time to perform.[28]

After the analysis of the biological human brain, it is observed that the parallel model of the human brain is the one where all signals from various other parts of the body come together and aggregate in a simultaneous manner[29].

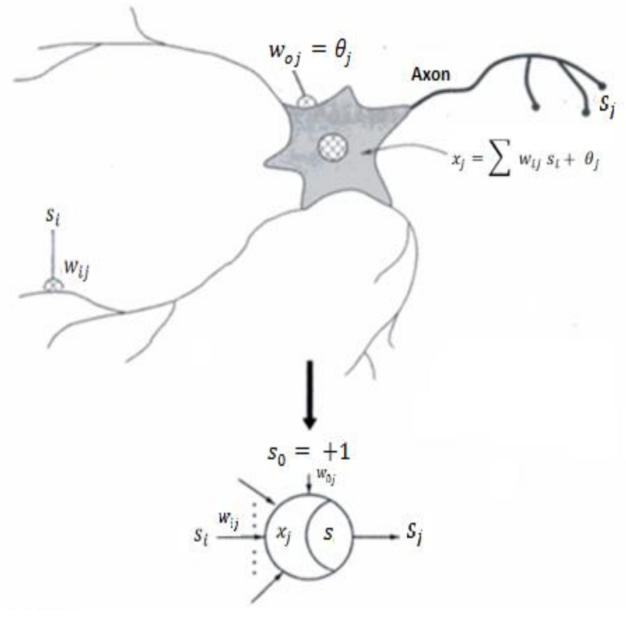

Fig.4 Mathematical model of a neural network

The mathematical expression of such a model can be given by:

$$y = f(\sum_{i=1}^{n} XiWi \ + \ \Theta) \qquad (7)$$

Here Xi signifies the signals obtained from various ways, Wi denotes the weight corresponding to a particular path and Θ is the bias of the network. [30]

Encryption using Chaotic Neural Network

The chaotic neural network implementation of the encryption mechanism is also a wide scope of research and future advancement. The basics of this concept originate from the statement of chaos theory put forth by Robert May [31].

Chaos can be understood as concept where there is a fixed output obtained for a fixed input in the system, but changes and variations in the input gives a totally different output that indicates of non-existent fixed mapping among the parameters of input and output of the stated system. Hence the system is adaptive to the changes in the inputs and gives output accordingly.[32]

The above condition can be illustrated as below:

$Y(i) = f^{n}(X(i)) \qquad \forall \quad X(i);$ (8)

But Y (i) is random for X (i+Δ);

where Δ stands for a change in X.

The aforementioned mathematical conditions are employed to get a **'chaotic neural network'** i.e. a neural network possessing the property of chaos [33]. The existence of chaos in the neural network signifies that the network model can vary dynamically according to the changes or variations in the respective input of the network. The condition is mathematically stated as [34]:

$W(i) = f'(X(i));$ (9)

here f ' is the function that changes the weights and model structure of the network model incessantly. The structure and behaviour of the neural network also keeps changing and showing variations in accordance to the varying weights of various paths. Thus it makes it impossible and infeasible for attackers and intruders to predict the exact nature or status of the network at any given time, given the fact that the network keeps changing all the time [35].

The different activation functions that get employed to design the chaotic neural networks are outlined as under:

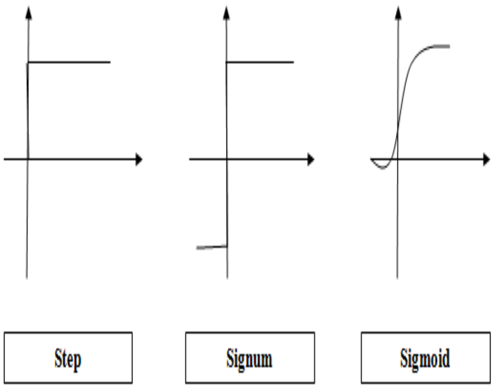

Fig.5 Different Activation Functions

III. TYPES OF NOISE

The noise is kind of a degradation of the digital image. As the digital images are subjected to various forms of processing, transformations, rampant usage and retrieval mechanisms.[36]

Image noise can be categorized as follows:-

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

A. *Gaussian Noise (Amplifier Noise)*

It is the form of electronic noise also called the amplifier noise because it originated from the amplifier in the devices of image capture, store and retrieval. This noise does not depend on the gray scale of the pixels of the image. It possesses a low power spectral density [27].

B. *Salt & pepper Noise (Impulse Noise)*

It is also called impulse noise or spike noise attributing toits impulsive behaviour. This noise appears to be in black and white spots that correlate to the look of the salt and pepper particles. This take only two values that are discrete in nature according to the salt and pepper.

C. *Speckle Noise (Multiplicative Noise)*

This noise follows a multiplicative pattern and the best pixel value that is effective is the real pixel measure with the noise coefficient multiplied with original pixel value

$$J = I + n*I. \qquad (10)$$

Here J stands for the speckle noise distribution and I is the original image.

D. *Poisson Noise (Shot Noise)*

- Also called the shot photon noise happens because of incapability of the image sensors to capture the true pixel in the proper manner to properly represent the picture [38].

IV. PREVIOUS WORK

This section presents the previous work in the domain.

This section deals with the significant contributions of the previous work in the particular area of research and their pros and cons. The limitations in each of the approaches has been clearly highlighted which forms the problem formulation.
Hao-Tian Wu et al. [1] proposed homomorphic encryption for images. Images were converted to the homomorphic image format with the image being a function of two components which are the reflectance and the illumination co-efficient values. The Paillier encryption mechanism is used in the approach to encrypt the data. The performance of the proposed system was evaluated in term so the peak signal to noise ratio. The variation of the peak signal to noise ratio was analyzed as function of the embedding rate. The major challenge with the proposed work was the fact that it did not have any separate or dedicated noise removal technique to

enhance the noise immunity of the images. Moreover, the encryption mechanism did not exhibit significantly high amounts of chaos which makes cryptosystems more immune to brute force attacks.

K.H.Jung [2] proposed a technique based on Data hiding in images using Pixel Value Difference (PVD) and Block Expansion technique. In this approach the interpolation operation has been used to find the expansion of the blocks of the pixels which the pixel difference is minimal and then the values of the blocks are utilized for data embedding. The major challenge with this approach of interpolation is the fact that interpolation and block expansion approaches may often lead to loss of data and resolution. This can be seen in the manifestation of the low value of the peak signal to noise ratio of the system and the relatively high value of mean square error of the system.

Somendu Chakroborty et al. [3] proposed the LSB injection technique for performing image steganography. The approach used the technique to convert the image into an LSB-MSB decomposition to find the co-efficient values which had the least amount of significant data and the values which have the maximal amount of significant data. The major challenge with such approaches is to figure out how to discriminate among the values of the co-efficient values which have MSBs and the ones which have the LSBs. The embedding of data in the transform domain is effective however it has the disadvantage of the data loss during the approximations in the transform and inverse transform process. This again manifests in the increase error profile of the extracted data.

K.Mohammad et al. [4] proposed blind spectral deconvolution using the Split Bregman approach for the restoration of images. This technique also introduced the use of the Wavelet Transform for the reconstruction of hyperspectral images. In the approach the wavelet co-efficient values are used for image restoration. This is done by the iterative decomposition of the image and discarding the detailed co-efficient values of the image. The main challenge of the image restoration in the transform domain is the fact that the image transforms and inverse transform pairs often introduce irrecoverable changes in the images which render loss of resolution in the image. This may often be effective in remove the noise and blurring effects in images but are not effective enough to simultaneously retain the image characteristics of the image to maintain quality.

H.Dadgostar et al. [5] developed an interval-valued intuitionistic fuzzy edge detection technique for conducting steganography and data embedding in images. The approach showed that the interval-valued approach for detecting images LSBs is effective for injecting or embedding secret data. The use of fuzzy logic was used as an expert view based system which would decide the places or blocks where the data can be embedded to make it least perceptible to the attackers. The major disadvantages with the fuzzy based approaches for data embedding is the fact that it is often extremely complex and non-deterministic to frame the membership functions for the cryptosystem as the fuzzy system needs to be trained with sufficient large amounts of data to be able to find the accurate ranges of the membership functions.

Xinvi Zhou et.al. [6] proposed LSB based color image steganography considering effects of noise. In this approach it was shown that the images are often degraded in their resolution, correlation co-efficient values and peak signal to noise ration due to the effect of noise and disturbances. The typical noise effects which affect the images are the Gaussian noise, the speckle noise, salt and pepper noise and Poisson noise. The noise removal mechanism has to be effective enough to just remove the noise and result in image quality degradation to as least a value as possible. The residual values of noise and disturbances can be evaluated in terms of the signal to noise ratio of the image.

Bin Li et al. [7] developed clustering modification for the purpose of spatial image data hiding applications. The approach tried to apply clustering to find out the redundant information of the images. It was shown that images in general have a lot of redundant data in the form of the pixels which clearly manifests itself when the image spectral analysis is done. The spectral analysis clearly shows that a lot of the pixels render information about the common spectral bands and hence cause large redundancies. This can cause the image to take up larges space in the memory for storage and also require more bandwidth for transmission. Another con is the requirement of more time and space complexity for the image processing applications.

Bi Li et al. [8] implemented spatial image steganography considering the effects of noise and disturbances. The spectral steganography approach is applicable to images which exhibit typical spectral redundancies and noise effects. It was shown that the several factors which lead to noise injection in the images are typically environmental factors, electronic equipment factors, storage and transmission factors etc. It was shown that it is necessary to alleviate the effects of noise and disturbances so as to enhance the quality of the image. While complete removal of the noise and disturbance effects was not possible to be done, however it was possible to implement recursive approaches to reduce the noise and degradation effects.

Mansi S at al. [9] presented a comprehensive survey on the pertaining issues on the data hiding and steganography of digital images. It could be summarized without loss of generality that image encryption is more perceptible to attackers and hence more prone to attacks as compared to image data hiding or steganography. The data hiding technique is generally shown to be more immune to attacks and hence more viable for maintaining attack immunity. This being said, it is also challenging to decide the spaces of the pixel values where the secret data is to be injected or embedded. The embedding rate should be high enough to practically embed high amounts of data while making the cover image with embedded data imperceptible to the attackers. The ease with which the data can be extracted is also critical. The various technique discussed are the steganography in transform domain, the spectral approach to steganography and the LSB injection. It was shown that the evaluation of such systems would be possible based on the evaluation parameters estimating the residual noise, errors and the signal strength of the image in comparison with the noise effects.

V. Holub et.al. [10] primarily focused on the image noise filtering applications which would help to root out the effects of the blurring and noise effects from images which are encrypted or which are used for data injection. The focus was on the design on the blind deconvolution model which would design the noise and degradation effects and then devise the image restoration process. The effective techniques which were discussed were the Lucy Richardson algorithm comprising of the blind deconvolution approach. The Wiener filtering approach was also analyzed and compared to the other image restoration filter techniques..

V. PERFORMANCE INDICES

The Peak Signal to Noise Ratio (PSNR) and mean square error (MSE) are two major deciding parameters in the effect of degradation of the image. While MSE is an amount of the errors in the image with respect to the original image, PSNR signifies the effect of residual noise

Mean Square Error (MSE)

The MSE represents the cumulative squared error of the original image and the extent to which image has transformed.

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 Ration (PSNR) tells about the amount of residual noise existing in the concerned image. The higher the value of signal power and the lower the value of the image power, higher is the PSNR measures. Peak Signal to Noise Ratio is usually expressed in decibels. It is mathematically expressed as below:

$$PSNR = 10log_{10}\frac{size^2}{mse} \qquad (11)$$

Here size stands for the size of the image

A high value of PSNR is indicative of that residual noise being existent in the image and needs to be removed by some filtering method.

Conclusion:

It is therefore conlcuded that the images that are digital in nature can be safeguarded by encyrption. For this, various encryption methods can be employed that have their own corresponding ros and cons.The crucial areas for consideration include space and time complexity and mesure of randomness .The use of robust and complex mathematical algorithms can make the system very robust and make it very arduous for the intruders to breach the system that renders the model efficient in tackling breaches. In adddition to it,the noise degradation in an area that need concern. The minimization of the noise effects requires to be done using appropriate methods. The MSE and PSNR are two important parameters that illustrate the efficacy of the algorithm.

REFERENCES

[1] H.T.Wu, Y.M.Cheung, Z.Yang, S.Tang, "A high-capacity reversible data hiding method for homomorphic encrypted images", Journal of Visual Communication and Image Representation, Vol-62, Elsevier 2020

[2] K.H. Jung, "High-capacity reversible data hiding method using block expansion in digital images", Volume-14, Springer 2021

[3] Somendu Chokroborty, Anand Singh Jalal, Charul Bhatnagar, "LSB based non blind predictive edge adaptive image steganography", Volume-76, Issue-6, Springer 2020

[4] K.Mohammad, M.Sajid, I Mehmood "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks", Elsevier 2018

[5] H.Dadgostar, F.Afsari, "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB", Volume-30, Elsevier 2017

[6] Xinyi Zhou, Wei Gong, WenLong Fu, Liang Jin, "An Improved Method for LSB based color image steganography combined with cryptography", IEEE 2016

[7] Bin Li, Ming Wand, Xiaolong Li, Shunquan Tan, Jiwu Huang, " A strategy of clustering modification directions in Spatial Image Steganography", Vol-10, Issue-9, IEEE Transactions 2015

[8] Bi Li, M Wang, J Huang, X Li, "A New Cost Function for Spatial Image Steganography", IEEE 2014.

[9] Mansi S, Vijay H Mankar, "Current Status and Key Issues in Image Steganography: A Survey", Volume-13, Elsevier 2014

[10] Zhenxing Qian, Xinpeng Zhang, Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE 2014

[11] A Bakhshandeh, Z Eslami "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", Elsevier 2013.

[12] K Gu, G Zhai, X Yang, W Zhang, "A new reduced-reference image quality assessment using structural degradation model", IEEE 2013

[13] YW Tai, S Lin, "Motion-aware noise filtering for de-blurring of noisy and blurry images", IEEE 2012

[14] A. Kanso and M. Ghebleh, "A Novel Image Encryption Algorithm Based on a 3D Chaotic Map", Elsevier 2012

[15] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE 2011

[16] W Hong, TS Chen, HY Wu, "Reversible An improved reversible data hiding in encrypted images using side match", IEEE 2011

[17] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function", IEEE 2010

[18] Ismail Amr Ismail, Mohammed Amin and Hossam Diab, "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps", International Journal of Network Security 2010

[19] CK Huang, HH Nien, "Multi chaotic systems based pixel shuffle for image encryption", Elsevier 2009

[20] R Rhouma, S Meherzi, S Belghith, “OCML-based colour image encryption”, Elsevier 2009

[21] T Gao, Z Chen, “A new image encryption algorithm based on hyper-chaos”, Elsevier 2008

[22] KW Wong, BSH Kwok, WS Law, “A fast image encryption scheme based on chaotic standard map”, Elsevier 2008

[23] Reversibility improved data hiding in encrypted Images,
Weiming Zhang, Kede Ma, Nenghai Yu, Elsevier, 2013

[24] 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

[25] Color image encryption using spatial bit-level permutation and high-dimensionChaotic system, Elsevier 2011 Hongjun Liu , Xingyuan Wan

[26] 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

[27] A novel colour image encryption algorithm based on chaos, Elsevier 2011
Xingyuan Wangn, Lin Teng, Xue Qin

[28] A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Elsevier 2011

[29] Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding, Elsevier2012 Zhengjun Liu, She Li, Wei Liu, Yanhua Wang, Shutian Liu

[30] A symmetric image encryption algorithm based on mixed Linear–nonlinear coupled map lattice, Elsevier 2014 Zhang Ying-Qian, Wang Xing-Yuan

[31] 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

[32] [10] A novel chaotic block image encryption algorithm basedon dynamic random growth technique, Elsevier 2014Xingyuan Wang, Lintao Liu, Yingqian Zhang

[33] 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

[34] 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

[35] Comparative Study of Different Noise Models and Effective Filtering Techniques,International Journal of Science and Research (IJSR)Dr. Aziz Makandar, Daneshwari Mulimani, Mahantesh Jevoor

[36] Efficient Technique for Colour Image Noise ReductionC.Mythili, V.KavithaThe Research Bulletin of Jordan, ISWSA;ACM 201

[37] Cryptography and Network Security, by Willaim Stallings, Pearson India.

[38] Digital Image Processing by Gonzalez and Woods, Person India.