IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 5 Issue 6 June, 2017

Image Encryption Using Dynamic Pixel Transformation under Effects of Blurring and Noise

Nidhi Sharma
M.Tech Scholar (Deptt. of CSE)
Vedica Institute of Technology,
RKDF University, Bhopal
Sharmanidhi2791@gmail.com

Akhilesh Bansiya
Asst. Professor (Deptt. of CSE)
Vedica Institute of Technology,
RKDF University, Bhopal
Akhilesh2483@gmail.com

ABSTRACT: Image encryption has become one of the most sought after areas of research recently due to the widespread use of digital images in various platforms and application ranging from web services, social media to defence etc. The focus lately has shifted to lightweight algorithms that do not exhibit high space and time complexity. Moreover, due to the digital transmission of images, they are also degraded by effects of blurring and noise. Hence it becomes mandatory to devise a mechanism for the restoration of degraded images. The presented paper focuses on both image encryption and decryption along with image restoration (removal of blurring and noise). The performance metrics have been chosen as Mean Square Error, Peak Signal To Noise Ratio and Throughput. MATLAB is used as a simulation tool for the results.

Keywords: Digital Image Processing (DIP), Image Denoising, Peak Signal to Noise Ratio (PSNR), Mean Square Error, Adaptive Pixel Masking.

I. Introduction

Cryptosystems have always been an area of active research to secure confidential and classified data. As digital technologies have taken over, digital images have become widespread in their applications. With a distinct difference in the information content in digital images compared to normal text data, encryption of digital images have evolved from conventional techniques to adaptive and light weight techniques for applications that can run on systems with moderate to low computational capacity. An **image** is a function of two variables and can be defined as *f(x,y)* where x and y are the coordinates in space on which the image values depend. Image pixel values often convey the following information:

1) The brightness at a point or the Gray Scale Value.
2) The color or frequency aspect of the point often referred to as the RGB value.
3) The co-ordinates of a point also convey the spatial information i.e. the values (x,y)

II. Fundamentals of Image Encryption

What is critical to save classified images form attacks is the algorithm that is used to encrypt it. While classical algorithms such as AES[3] or Blowfish[3] do perform the task at hand, but the internal architecture of such algorithms is well known which lets attackers exploit even slightly visible trends in the encrypted image. A second binding factor is the fact that these algorithms were designed typically for textual data which means that the arrangement or permutation of the pixels or picture elements is immaterial. This causes degradations in the image even after decryption. Thus these techniques need considerable amount of space and time complexity to handle digital images. A much sought after algorithm is one in which the values of key and algorithmic parameters change dynamically with the change in the image to be encrypted. Such a technique masks the desired pixels adaptively and can be termed as **Variable Pixel Transformation.** The aim of such an algorithm is to design high amount of randomness in the image and also make the algorithm light weight so as to make it practically feasible for widespread applications.

III. DEGRADATION MODEL FOR DIGITAL IMAGES

Digital images undergo several types of degradations while storage and transmission through channels. The most common sources of noise and blurring effects affect the image under consideration while passing through the communication medium which is termed as the channel or while storage in electronic storage systems. As the degradations are highly random in nature, therefore they are typically designated as random variables described by their statistical parameters. It is crucial that we know about the statistical parameters of the degradations so that we can revert the effects caused by the sources. Thus we need to have the degradation model design for removal of the detrimental effects.

SOURCES OF NOISE AFFECTING DIGITAL IMAGES

Several sources of noise affect signals passing through the communication media or the channel. Our interest lies in that noise and blurring mechanisms that degrade digital images the most. A description of the same is given below.

COMMON NOISE TYPES AFFECTING DIGITAL IMAGES

As described earlier, the different noise types which degrade images are given below. It should be noted though that they are characterized by their statistical properties.

1) Gaussian Noise
2) Speckle Noise
3) Salt and Pepper Noise
4) Poisson Noise.

Gaussian Noise

It is typically encountered in electronic amplifier systems which are essential for boosting the strength of the image signals while they wean down.

Gaussian Noise is described statistically by its:

1) Mean
2) Variance

Salt & pepper Noise or Impulsive Noise

It is encountered majorly in the inbuilt analog to digital converters or ADCs in the devices that convert the analog information into digital information. It can be caused by inappropriate or corrupt values of the picture elements or pixels. It can also be caused by spikes of currents or surges in voltage in the ADCs.

Salt and Pepper Noise is statistically described by its:

1) Mean
2) Variance
3) Noise Density

Speckle Noise or Multiplicative Noise

It exhibits a multiplicative nature wherein the original image values are M and the one after the impact of noise is M'

$M' = IM + k*M$

It can be seen that the noise would have a high effect for higher values of M or for a simultaneous high value of 'k'.

It is statistically described by the following statistical parameters:

1) Mean
2) Variance
3) Noise Density

Poisson Noise or Shot Noise.

It is encountered if the sensor capturing the digital image gets lesser number of pixel values than what is necessary for it. The absence of such pixel values often a noise termed as Poisson noise which follows the Poisson distribution for the noise random variable.

It is statistically described by:

1) Variable Mean or expectation value
2) Value of Standard deviation or value of variance.

IV RESTORING DIGITAL IMAGES EMPLOYING LINEAR FILTERING

Images undergo several random degradations such

as noise and blurring effects. Although the effects are random in nature, yet they can be modelled statistically using parameters such as mean, variance, standard deviation etc.[7]Its essential though that the restoring mechanism does not introduce non-linearity of its own. Hence is judicious to use linear filtering such as the Wiener filter which exhibits a highly linear nature.

Such a mechanism can be described as:

$y(t)=x(t)*\{n(t)+b(t)\}$

Here y(t) is the output of the filter in time domain, x(t) is the input to the filter in time domain, n(t) is the noise function and b(t) is the blurring function.

V. SYSTEM DESIGN.

Variable Pixel Transformation is mathematically modelled as:

1) Load Image that is to be encrypted and let it be denoted by X
1. Get the dimensions describing the size of the image. Store them and term them as (i, j, k).
2. X→ g(i,j,k) where g denotes the function describing dependence of the original image of (i,j,k).
3. Now, based on the values obtained above i.e. (i,j,k), design an adaptive key generating mechanism that would yields different keys as the image values (i,j,k) change
4. Let such as key be Key=h(i,j,k) where h is the mathematical function for key generation
5. Based on the obtained values of the image parameters and the key values, design an encryption mechanism that would adaptively change with the change in encryption mechanism designated by the transformation: Y→z'(I, Key).
6. By defining the statistical values of the blurring and noise effects, the Image Degradation Model has been designed.
7. With Degradations in the image after defining the values, the next task is to display image.
8. By assuming zero NSR, we have to apply filter with degradation statistical parameters.
9. After the above analysis the noise would be removed this is called de-noising.
10. With the help of key and decryption algorithm the image can be recovered. Compute
11. At last we evaluate Parameters such as Mean Square Error, PSNR and Throughput.

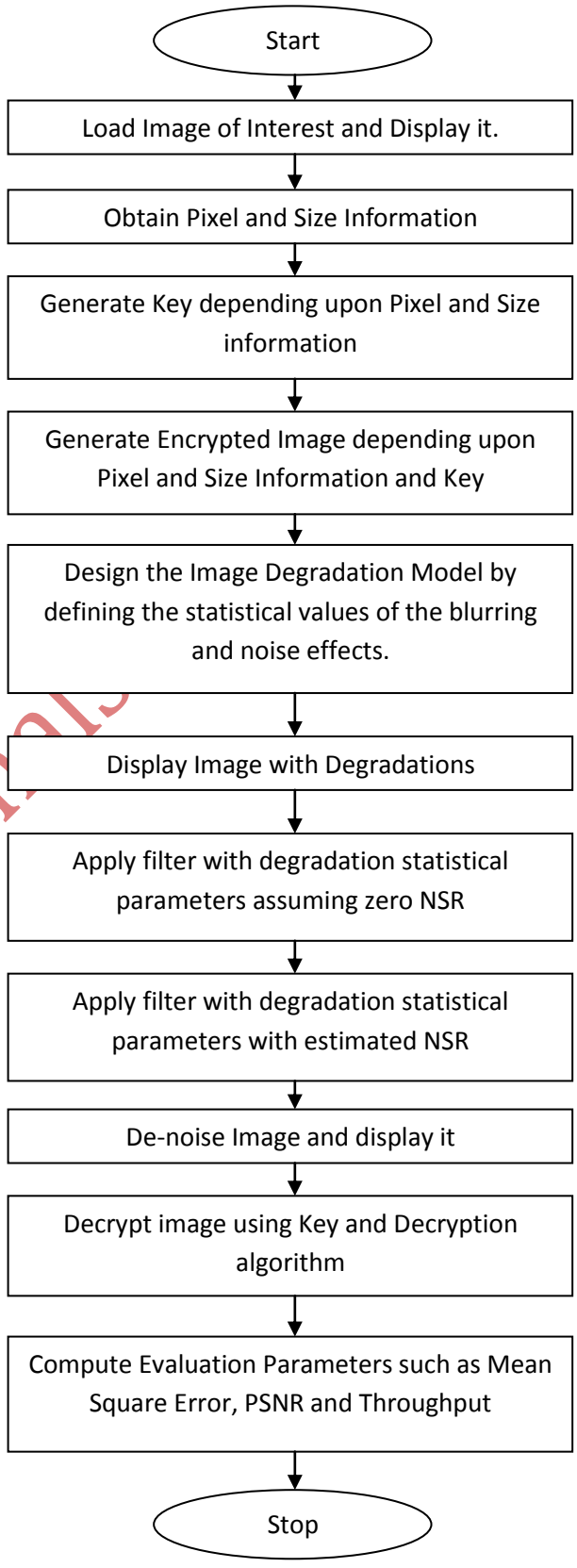

Fig.1 Proposed Flow Diagram

The most fundamental requirement of the image encryption model is the variation or changes in the key and the encryption mechanism in accordance with the changes or variations of the image under interest. In the proposed technique, the key depends on the image under consideration and the image encryption mechanism that also depends on the key changes with the change in the image. Thus, and variation in the input of the designed system brings about a manifold change in the output of the same system. This effect is also called the **Avalanche Effect** in cryptosystems. Higher avalanche makes potential threats difficult.

It should be noted here that z' should be comprised of functions which use bitwise XOR, or prime logarithms or modular arithmetic which exhibit a trapdoor approach and becomes infeasible to break by brute force.

VI. ANALYSIS OF OBTAINED RESULTS

The test images taken for this study are len.jpg and cameraman.jpg. Results obtained using the proposed algorithm has been shown below.

Fig. 1 Test Image 1
Fig. 2 Test Image2

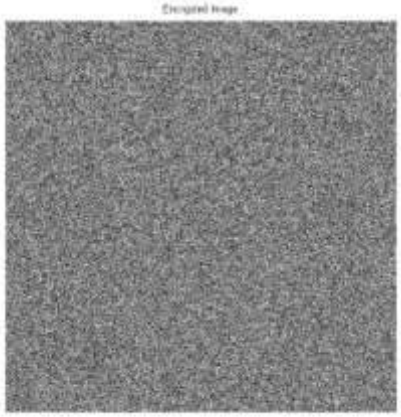

Fig.3 Image Encrypted using Proposed Algorithm

Fig.3 Effect of Blurring on Image

Fig.4 Effect of Blurring and Gaussian Noise

Fig.5 Restored of Degraded Image AssumingZero Spectral Noise

Fig.6 Effect of Blurring and Salt & Pepper Noise

Fig.7 Effect of Blurring and Speckle Noise

Fig.8 Effect of Blurring and Poisson Noise

Fig.9 Restoring Image after Estimating the Noise Power in Spectrum of Image

Fig.10 Final Decrypted Image

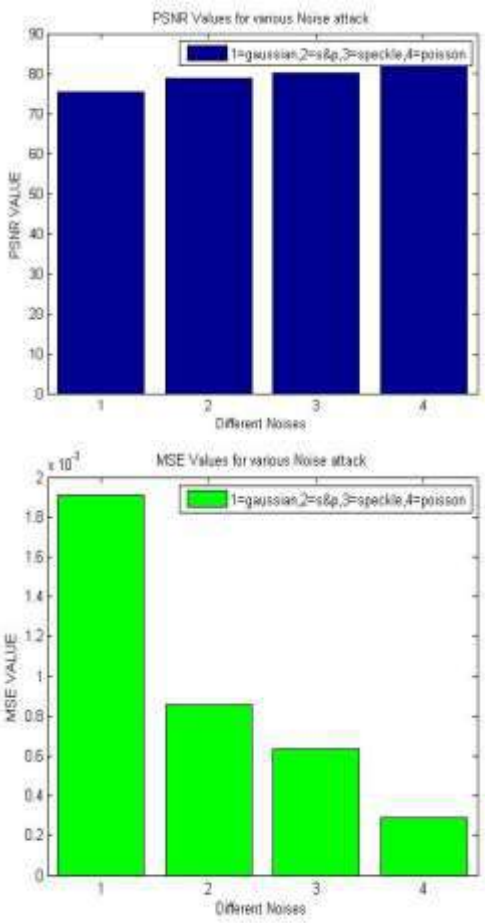

Fig.11 PSNR Values for Different Noise Effects

Fig.12 MSE Values for Different Noise Effects

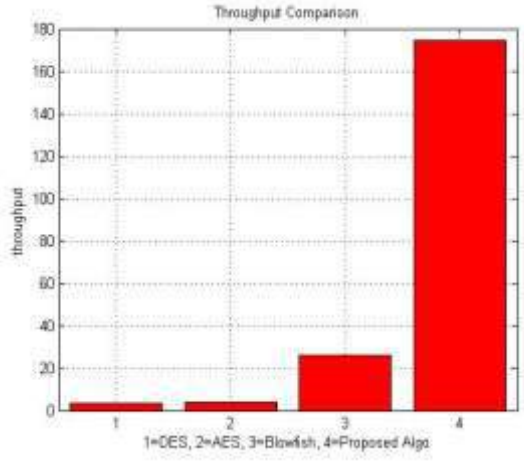

Fig.13 Comparative Throughput for Standard Encryption Algorithms

Fig.14 GUI for Cameraman.jpg
Fig.15 GUI for Lena.jpg Comparative PSNR Analysis of Base Paper and Proposed Work

Image: Lena		
S.No	**Paper**	**PSNR Value**
1	**Securing the Architecture of the JPEG Compression by an Dynamic Encryption, Faik GMIRA et.al**	**34.3417**
2	**Proposed Work**	**75.3500**

Image: Cameraman		
S.No	**Paper**	**PSNR Value**
1	**Securing the Architecture of the JPEG Compression by an Dynamic Encryption, Faik GMIRA et.al**	**31.0252**
2	**Proposed Work**	**74.3893**

Conclusion:

Here we have presented an algorithm that adapts itself to the changes in the plaintext image in terms of the key and the encrypting parameters. The different degradation mechanisms such as noise and blurring effects have been simulated. Image restoration has also been achieved using linear filtering. It has been shown that the proposed algorithm achieves better value of PSNR, MSE and throughput compared to standard encryption algorithms. A high value of throughput indicates the fact that the algorithm is a light weight algorithm which can be used on computational platforms having limited computational competence.

References

[1] Nidaa AbdulMohsin Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map",Elesvier ,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

[13]F.Menichelli, R. Menicocci, M. Olivieri and Alessandro Trifiletti, "High Level Side Channel Modeling and Simulation for Security Critical Systems on Chips", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp. 164-175, 2008.

[14]E. Bertino, N. Shang and S. S. Wagstaff, "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 2, pp. 65-70, 2008.

[15] Sudharsanan S, "Shared Key Encryption of JPEG Color Images", IEEE Transactions On

Consumer Electronics, Vol. 51, No. 4, November 2005

[16] Johnson M, Ishwar P, Prabhakaran V, Schonberg D, and Ramchandran K, "On Compressing Encrypted Data", IEEE Transactions On Signal Processing, Vol. 52, No. 10, October 2004

[17] Bharat B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan and K.S. Trivedi, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems", Journal of Performance Evaluation, Elsevier Science Publishers, Vol. 56, No. 1, pp. 167-186, 2004.

[18] Parminder Kaur and Jagroop Singh. 2011. A Study Effect of Gaussian Noise on PSNR Value for Digital Images International Journal of Computer and Electrical E ngineering.Vol. 3, No.2, 1793-8163.

[19] Mrs. C. Mythili and Dr. V.Kavitha. Efficient Technique for Color Image Noise Reduction T h e R e s e a r c h B u l l e t i n o f J o r d a n ACM , V o l . I I (I I I)

[20] Mr. Amit Agrawal and Ramesh Raskar. Optimal single image capture for motion deblurring. In Proc. IEEE Conference on Computer Vision and Pattern Recognition, pages 2560{2567, 2009.

[21] Mr. Pawan Patidar and et al. Image De-noising by Various Filters for Different Noise in International Journal of Computer Applications (0975 – 8887) Volume 9– No.4, November 2010

[22] Charles Boncelet (2005)."Image Noise Models". in Alan C.Bovik. Handbook of Image and Video Processing.

[24] Mr. Salem Saleh Al-amri and et al. Comparative Study of Removal Noise from Remote Sensing Image. IJCSI International Journal of Computer Science Issues, Vol. 7, Issue. 1, No. 1, January 2010 32 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814

[25] C. P. Su, T. F. Lin, C. T. Huang and C. W. Wu, "A High-Throughput Low Cost AES Processor", IEEE Commun.

