Image Encryption using Adaptive Pixel Masking under Various Noise Attacks

Garima Pal
M.Tech Scholar
LKCT, Indore
India

Vijay Kumar Verma
Asst.Professor
LKCT, Indore
India

ABSTRACT
Cryptosystems have always had tremendous applications in the fields of data security. With ever growing applications of digital images, encryption of images has emerged as a highly sought after area of research. In this present paper, a novel adaptive pixel masking scheme has been introduced for image encryption. Since images undergo degradations while transmission as well as storage, an image degradation model has been designed and simulated for common types of noise and blurring effects. Further a technique comprising of linear filtering has been proposed. It has been shown that the proposed technique achieves improved results in terms of Peak Signal to Noise Ratio and Mean Square Error as compared to previous works. A detailed description of the aforesaid aspects ensues.

General Terms
Image Encryption, Adaptive Pixel Masking, Noise Attack, Image Restoration.

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

1. 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 of (x,y)

2. IMAGE ENCRYPTION USING ADAPTIVE PIXEL MASKING
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 **Adaptive Pixel Masking.** 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.

3. DEGRADATION MODEL FOR DIGITAL IMAGES

3.1 Image Degradation
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.

3.2 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.

3.3 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 is described statistically by

1) Mean
2) Variance

Salt & pepper Noise or Impulsive Noise

It is encountered majorly in the in built 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.

It is statistically described by;

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.

4. 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 modeled 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.

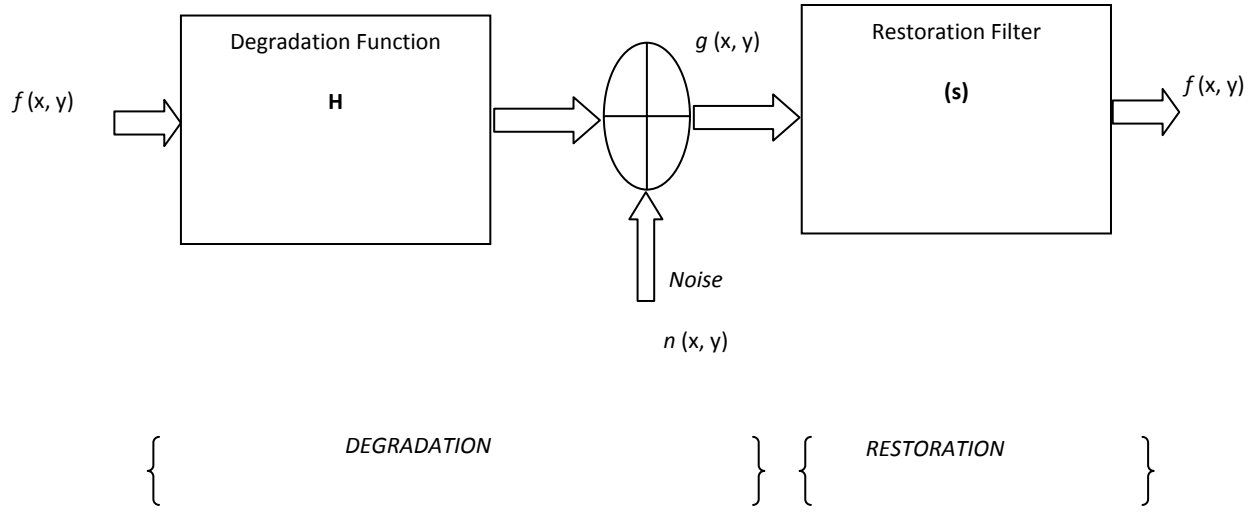

Fig 1: The Image Degradation Model

5. SYSTEM DESIGN

Adaptive Pixel Masking 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 vales 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:

   $Y \rightarrow z'(I, Key)$.

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.

6. RESULTS

Results obtained using the proposed algorithm has been shown below.

Fig.2: Original Image

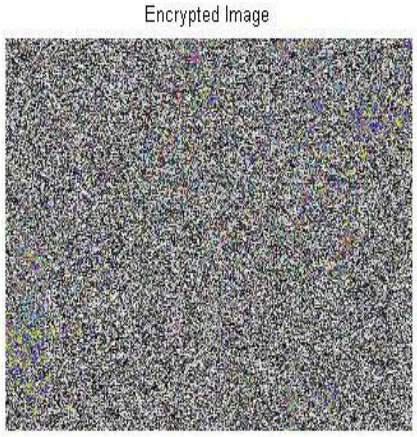

Fig.3: Image Encrypted using Proposed Algorithm

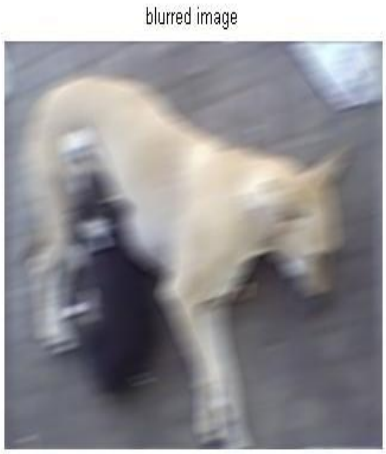

Fig.4: Effect of Blurring on Image

Fig.5: Effect of Blurring and Gaussian Noise

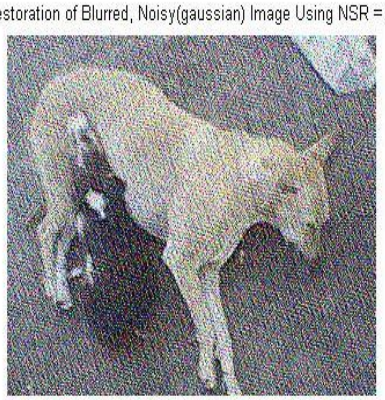

Fig.6: Restored of Degraded Image Assuming Zero Spectral Noise

Fig.7: Effect of Blurring and Salt & Pepper Noise

Fig.8: Effect of Blurring and Speckle Noise

Fig.9: Effect of Blurring and Poisson Noise

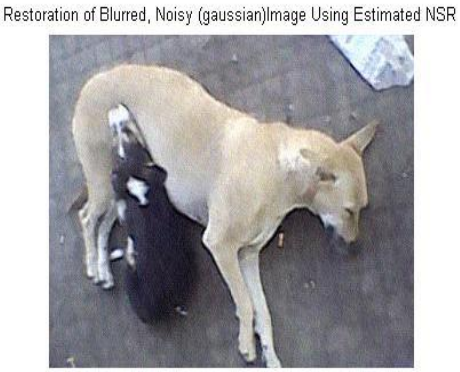

Fig.10: Restoring Image after Estimating the Noise Power in Spectrum of Image

Fig.11: Final Decrypted Image

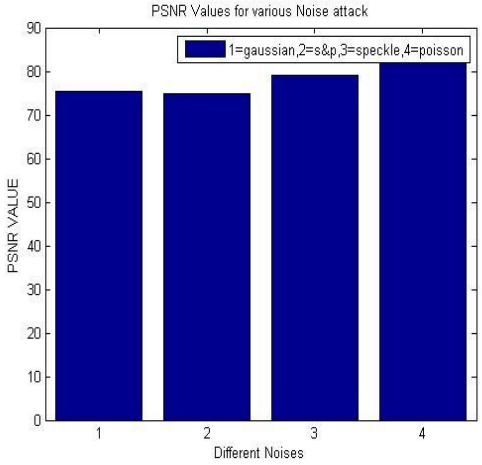

Fig.12: PSNR Values for Different Noise Effects

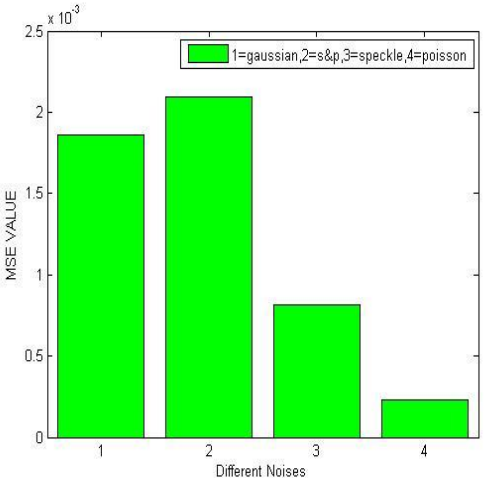

Fig.13: MSE Values for Different Noise Effects

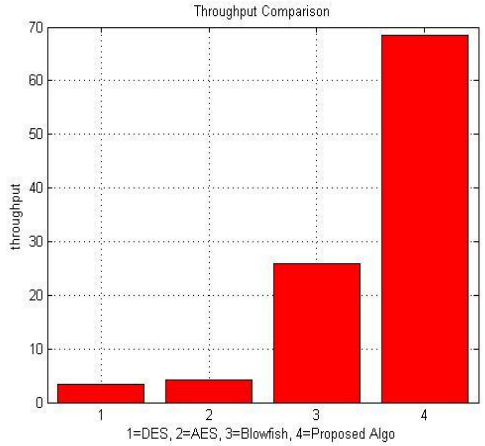

Fig.14: Comparative Throughput for Standard Encryption Algorithms

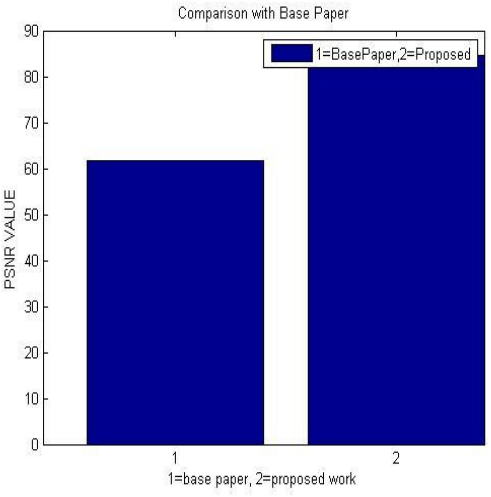

Fig.15: Comparative PSNR analysis with Base Paper (Weiming Zhang et.al, [2])

7. CONCLUSION

Here an algorithm has been proposed 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. It should be noted that further improvements or future enhancements of the proposed work can be attaining multiple levels of encryption. Also image compression may also be considered so as to simplify the process of data storage and transmission.

8. ACKNOWLEDGMENTS

I would like to convey my sincere and heartfelt to thanks to Mr. Vijay Kumar Verma and Dr. Sanjay Thakur for their continued guidance, motivation and support. Without their contributions, this research work wouldn't have seen the light of the day.

9. REFERENCES

[1] Nidaa AbdulMohsin Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map",Elesvier ,2015.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] Reversibility improved data hiding in encrypted images, by Weiming Zhang, Kede Ma, Yu Elsevier 2014.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] Maniccam S.S., Bourbakis N.G., "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001) 1229-1245 Springer 2014Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[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

[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 Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender