

## Performance Evaluation of Digital Image Encryption Using Discrete Random Distributions and MOD Operator

H.B.Kekre<sup>1</sup>, Tanuja Sarode<sup>2</sup>, Pallavi N Halarnkar<sup>3</sup>

<sup>1</sup>(Computer Engineering, MPSTME/NMIMS, India)

<sup>2</sup>(Computer Engineering, TSEC/Mumbai, India)

<sup>3</sup>(Computer Engineering, MPSTME/NMIMS, India)

---

**Abstract :** Information security is important in all the domains. Image Processing is one such domain which has huge amount of information in the form of Digital images. To secure image data there are many ways, one of them is Image Encryption. In this paper we have presented a novel approach for Image Encryption. Randomness of Discrete Distributions along with MOD invertible operator is used for encrypting the image. A new Experimental parameter called as Peak Average Fractional Change in Pixel value is introduced. For analysis purpose, Image moments are also calculated

**Keywords:** Discrete Distributions, Image Encryption, Image Moments, Image Scrambling, PAFCPV

---

### I. INTRODUCTION

Information security and confidentiality is important at different levels of communication. The applications find their way into different fields like personal data, patient's medical data, military etc. With the advancement in Research in the field of Image processing, Image encryption and steganographic techniques have gained a popularity over the other forms of hidden communication. A new Image Encryption technique using Fibonacci and Lucas is proposed in [1]. The approach makes use of Arnold Transform matrix, and uses the generalized Fibonacci and lucas series values in the Arnold transform to scramble the image.

An encryption technique based on pixels is proposed in[2]. Firstly the image is scrambled using the method of watermarking making it difficult for decoding purpose. Lastly a camouflaged image to vision or the pixels of the true image to get the final encrypted image. The key parameters are encrypted using Elliptic curve cryptography (ECC). The algorithm security, reliability and efficiency is analyzed via experimental analysis.

A new invertible two dimensional map is proposed in [3] called as Line Map, for image encryption and decryption. The method maps the digital image to an array of pixels and then maps it back from array to image. A Line Map consists of two maps, a left map and a right map. The drawback of the traditional 2D maps which can be used only for permutation is overcome by Line Map which can perform two processes of image encryption , permutation and substitution simultaneously using the same maps. The proposed method does not have a loss of information, it is also fast and there is no restriction on the length of the security key.

Pawan et.al proposed a encryption technique for a color image in [4]. The method proposed makes use of 3D logistic map, 3D Chebyshev map, and 3D and 2D Arnolds cat map. 2D Arnolds map is used as a Image scrambler, which is extended to 3D for R,G,and B components. Key generation is done using 3D chebyshev map. Image scrambling is done by using 3D logistic map. The method proposed provides more security to digital images as both shuffling and substitution is provided in the approach. The Chebyshev map is used for public key encryption and distribution of generated private keys.

Image encryption is a method to provide more security to digital images. A new image cryptosystem is proposed in[5]. It has two main parts, encryption/decryption algorithm and ciphered key. The encryption process consists of two main steps diffusion stage and substitution stage. Diffusion stage makes use of the XOR operator. For substitution two encryption processes are used, Lagrange process and Least square process. For decryption the processes are just reversed to obtain the original image. Based on the initial key two different approaches are proposed, the first one makes use of a key whose length is 192bits (24 bytes) in hexadecimal system as its input and then the key is expanded using AES-192 key expansion algorithm. The second approach makes use of the image as a key to cipher the plain image.

Two new image encryption approaches are proposed in [6], one is based on spatial domain and the other on frequency domain. The proposed approach uses Fibonacci P-code, a parametric sequence. The parameter p is used as a key, which has many possible choices. The proposed method can be used for both full and partial image scrambling. The presented method is robust against common attacks like cutting(data loss), compression and noise. Lucas p-code is also introduced for image scrambling. The Fibonacci p-code is also compared with classical Fibonacci series.

A chaotic map has randomness, makes use of this randomness for shuffling the pixel positions based on the random positions generated. The proposed approach in [7] makes use of two different chaotic maps for the same. The maps used are Henon and Lorenz for pixel shuffling. The maps are also compared for performance.

Cyclic Elliptic curves with order M are used for designing symmetric key image encryption method. Random sequence of integers are generated using Linear Feedback shift register. Such sequences are called as maximal length sequences. The sequence is used for deriving several binary and non binary sequences which are useful in stream cipher systems. Two encryption algorithms are used Additive Cipher and Affine Cipher. The results of image encryption are shown over medical images in[8]

A combination of shuffling and encryption is proposed in [9]. The paper uses Arnold cat map for shuffling the pixel positions, then a Henon chaotic map is used to encrypt the shuffled pixel values. Experimental results show that the proposed method is efficient and secured in statistical analysis and key sensitivity tests. The distribution of image values show a random like behavior.

Many of the existing encryption methods may not be suitable for multimedia data like images. [10] proposes a block based transformation algorithm based on a combination of image transformation and a image encryption technique called as blowfish. Firstly image is divided into blocks, then the transformation is applied to each block, then the transformed image was encrypted using blowfish method. Experimental results show that correlation between the elements is reduced. The results also show that increasing the number of blocks decreases the correlation further thereby increasing entropy.

Around 14 different methods are compared in [11]. Spatial domain methods include 6 of them and transform based are the remaining. The comparison of these methods is done on different parameter like, tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, cryptographic security. In the comparison it is found that none of these methods satisfy all the parameters.

A new encryption technique called as Hyper Image Encryption Algorithm (HIEA) is proposed in [12]. A permutation process is applied over the binary values. The generated image after the permutation process will be encrypted using HIEA. Experimental parameters like encryption and decryption time and entropy is used for analysis.

A novel image encryption technique combining Julia sets and Hilbert curves is proposed in [13]. Julia sets are used to generate a random sequence as the initial keys and gets the final encryption keys by scrambling the initial keys using Hilbert curve. The final encrypted image is obtained by modulo arithmetic and diffuser operation. Experimental results show that the proposed method has large key space, good statistical property, high sensitivity for the keys and effective resistance to the chosen plain text attack.

Ahmad et.al presented a framework for different encryption schemes in [14]. Rather than visual inspection it makes use of number of parameters like correlation coefficient, information entropy, compression friendliness, number of pixel change rate, and unified average change intensity. These parameters are used to quantify the quality of encrypted images. Efficiency analysis and security evaluation of Advanced Encryption Standard(AES) and Compression Friendly Encryption Scheme(CFES) is also given. The brute force, statistical and differential attacks are explored for AES and CFES. Experimental results have shown some weaknesses to CFES with respect to entropy and horizontal correlation.

In this paper, Section II gives the details of Discrete Distributions used for generating Random numbers. Sections III explains how Random number can be generated using Discrete Distributions in Matlab. Section IV explains the scaling method used for scaling the random numbers generated in matlab using discrete distributions. Section V explains the MOD operator used for Image Encryption. Section VI explains the proposed approach. Section VII includes the experimental results obtained for the proposed approach and Section VIII states the conclusion.

## **II. DISCRETE DISTRIBUTIONS**

### **2.1 Discrete Random Variables**

Discrete random variables are characterized by their supports which take the form

$$S_x = \{U_1, U_2, U_3, \dots, U_K\} \text{ or } \{U_1, U_2, U_3, \dots\}$$

Every discrete random variable X has associated with it a probability mass function (PMF)

$$f_X : S_x \rightarrow (0, 1) \text{ defined by}$$

$$f_X(X) = \mathbb{P}(X=x), x \in S_x$$

Since values of the PMF represent probabilities, PMFs enjoy certain properties. In particular, all PMFs satisfy

1)  $f_X(x) > 0$  for  $x \in S$

- 2)  $\sum_{x \in S} f_x(x) = 1$
- 3)  $\mathbb{P}(X \in A) = \sum_{x \in A} f_x(x)$  for any event  $A \subset S$

**2.2 Image Moments : Mean, Variance, Standard Deviation, Skewness and Kurtosis**

Consider an image  $I_{ij}$  where  $i,j=0,1,2,\dots,255$ . The image moments mean, variance, std deviation, skewness and kurtosis are defined as follows

Mean:

$$\bar{X} = \frac{1}{N^2} \sum_{ij=0}^{255} I_{i,j} \tag{1}$$

Variance: It is measure of how far the numbers lie from mean.

$$\sigma^2 = \frac{1}{N^2} \sum_{ij=0}^{255} (I_{i,j} - \bar{X})^2 \tag{2}$$

Std Deviation: it is a measure of variability or diversity. It shows how much variation or dispersion exists from mean. A low value indicates the values tend to be close to mean whereas a high value indicates the values are spreadout over a large range.

$$\sigma = \sqrt{\sigma^2} \tag{3}$$

Skewness: it is a measure of the asymmetry of the probability distribution. The skewness can be positive or negative or even undefined

$$S_k^3 = \sqrt[3]{\frac{1}{N^2} \sum_{ij=0}^{255} (I_{i,j} - \bar{X})^3} \tag{4}$$

Kurtosis: It is measure of the shape of distribution. kurtosis as a measure of how flat the top of a symmetric distribution is when compared to a normal distribution of the same variance

$$K_k^4 = \sqrt[4]{\frac{1}{N^2} \sum_{ij=0}^{255} (I_{i,j} - \bar{X})^4} \tag{5}$$

Note: Higher Moments are not important as they can be derived from these four moments

**2.3 The Discrete Distribution**  
**Uniform Distribution**

A random variable  $X$  with the discrete uniform distribution on the integers  $1, 2, \dots, m$  has PMF

$$f_X(x) = \frac{1}{m}, x = 1,2, \dots, m \tag{6}$$

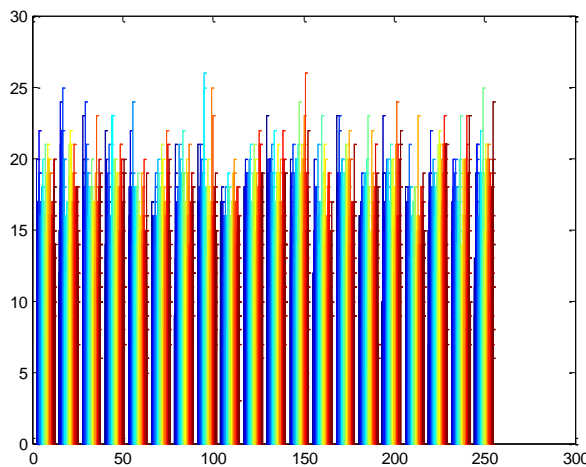


Figure 1. 2D Random Uniform Distribution

Figure 1. shows the 2D Random Uniform Distribution numbers generated using the inbuilt function of matlab.

**Binomial Distribution**

The Binomial distribution is based on a *Bernoulli trial*, which is a random experiment in which there are only two possible outcomes: success (*S*) and failure (*F*). We conduct the Bernoulli trial and let

$$X = \begin{cases} 1 & \text{if the outcome is } S \\ 0 & \text{if the outcome is } f \end{cases} \tag{7}$$

If the probability of success is  $p$  then the probability of failure must be  $1 - p = q$  and the PMF of  $X$  is

$$f_X(x) = p^x(1 - p)^{1-x}, x = 0,1, \dots \tag{8}$$

It is easy to calculate  $\mu = \mathbb{E}[X] = p$  and  $\mathbb{E}[X^2] = p$  so that  $\sigma^2 = p - p^2 = p(1 - p)$

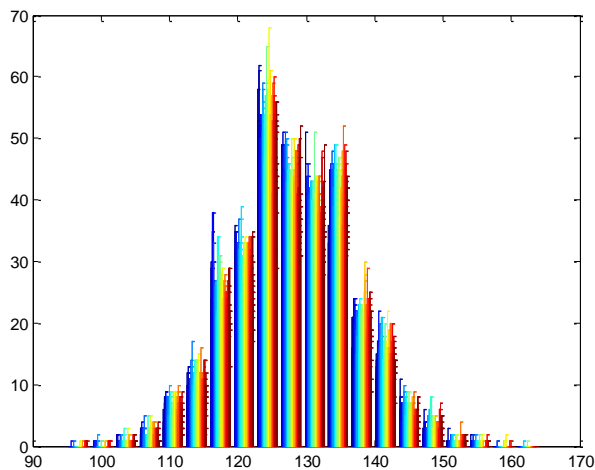


Figure 2.1 2D Binomial Random Distribution

Figure 2.1. shows the 2D Random Binomial Distribution numbers generated using the inbuilt function of matlab.

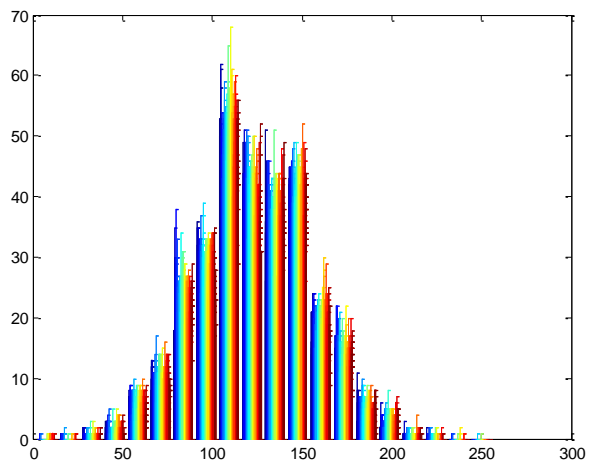


Figure 2.2 2D Binomial Random Distribution after scaling

Figure 2.2. shows the 2D Random Uniform Distribution numbers after applying the scaling method.

**Poisson distribution**

This is a distribution associated with “rare events”, for reasons which will become clear in a moment. The events might be:

- Traffic accidents,
- Typing errors, or
- Customers arriving in a bank.

Let  $\lambda$  be the average number of events in the time interval  $[0, 1]$ . Let the random variable  $X$  count the number of events occurring in the interval. Then under certain reasonable conditions it can be shown that

$$f_X(x) = \mathbb{P}(X = x) = e^{-\lambda} \frac{\lambda^x}{x!}, x = 0, 1, 2, \dots \dots \quad (9)$$

Divide  $[0, 1]$  into subintervals of length  $1/n$ . A *Poisson process* satisfies the following conditions:

- The probability of an event occurring in a particular subinterval is  $\approx \lambda/n$ .
- The probability of two or more events occurring in any subinterval is  $\approx 0$ .
- Occurrences in disjoint subintervals are independent.

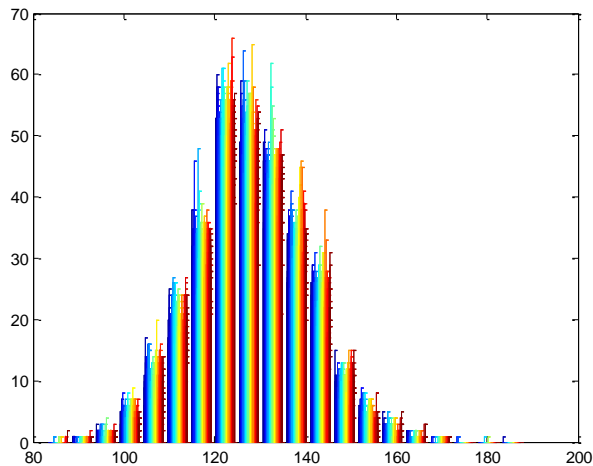


Figure 3.1 2D Poisson Random Distribution

Figure 3.1. shows the 2D Random Poisson Distribution numbers generated using the inbuilt function of matlab.

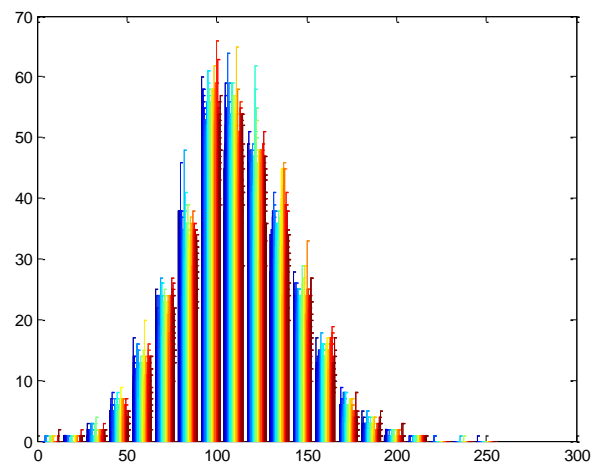


Figure 3.2 2D Poisson Random Distribution after scaling

Figure 3.2. shows the 2D Random Poisson Distribution numbers after applying the scaling function.

### Geometric Distribution

Another important class of problems is associated with the amount of time it takes for a specified event of interest to occur. For example, we could flip a coin repeatedly until we observe Heads. We could toss a piece of paper repeatedly until we make it in the trash can.

Suppose that we conduct Bernoulli trials repeatedly, noting the successes and failures. Let  $X$  be the number of failures before a success. If  $\mathbb{P}(S) = p$  then  $X$  has PMF

$$f_X(x) = p(1 - p)^x, x = 0, 1, 2, \dots \dots \quad (10)$$

X has a Geometric distribution

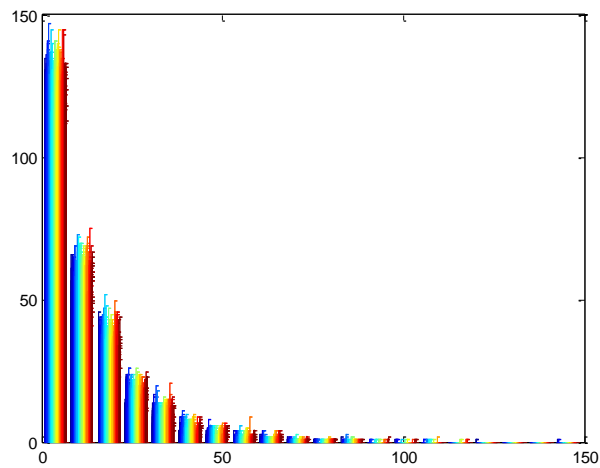


Figure 4.1 2D Geometric Random Distribution

Figure 4.1. shows the 2D Random Geometric Distribution numbers generated using the inbuilt function of matlab.

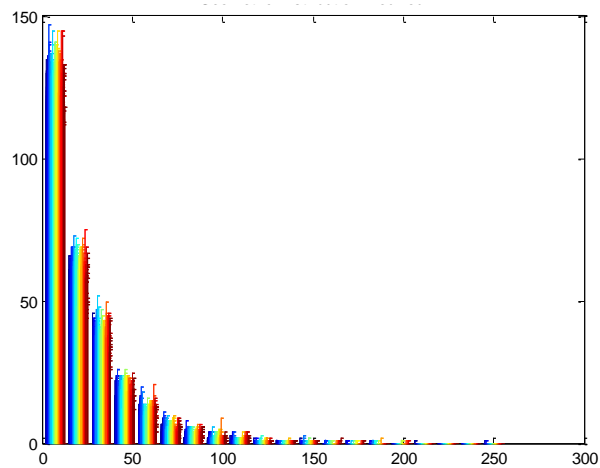


Figure 4.2 2D Geometric Random Distribution after scaling

Figure 4.2. shows the 2D Random Geometric Distribution numbers after applying the scaling function

### Hyper-Geometric Distribution

A Dependent Bernoulli Trials Distribution, called as Hypergeometric Distribution.

Consider an urn with 7 white balls and 5 black balls. Let our random experiment be to randomly select 4 balls, without replacement, from the urn. Then the probability of observing 3 white balls (and thus 1 black ball) would be

$$P(3W, 1B) = \frac{\binom{7}{3}\binom{5}{1}}{\binom{12}{4}}$$

More generally, we sample without replacement  $K$  times from an urn with  $M$  white balls and  $N$  black balls. Let  $X$  be the number of white balls in the sample. The PMF of  $X$  is

$$f_X(x) = \frac{\binom{M}{x}\binom{N}{K-x}}{\binom{M+N}{K}} \quad (11)$$

X is a Hypergeometric Distribution

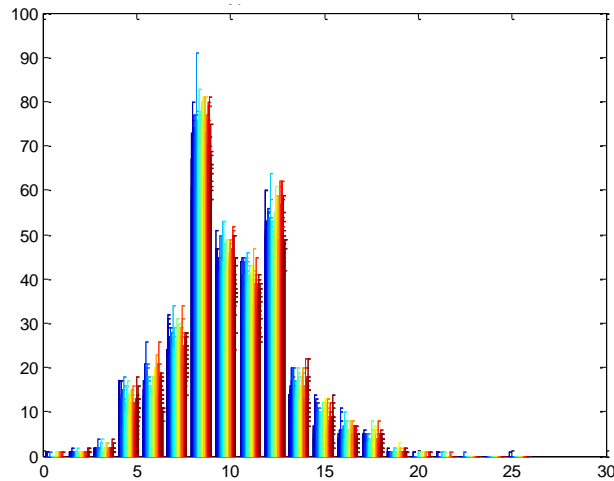


Figure 5.1 2D HyperGeometric Random Distribution

Figure 5.1. shows the 2D Random Hypergeometric Distribution numbers generated using the inbuilt function of matlab.

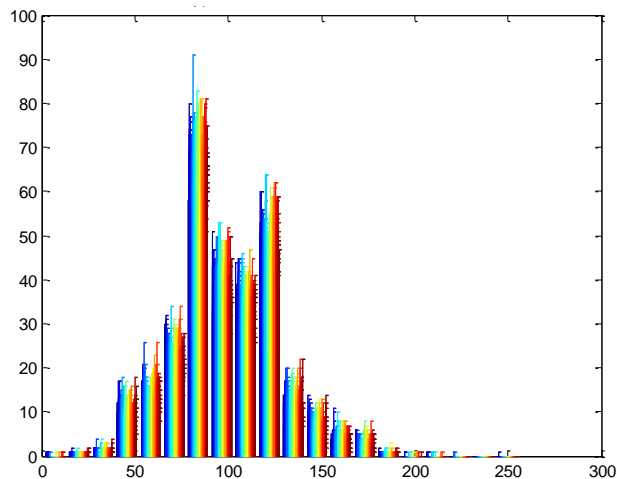


Figure 5.2 2D HyperGeometric Random Distribution after scaling

Figure 5.2. shows the 2D Random HyperGeometric distribution numbers after applying the scaling function

### III. RANDOM NUMBER GENERATION USING DISCRETE DISTRIBUTIONS IN MATLAB

Matlab Software is used to generate Random Numbers which are derived on the basis of Different Discrete Distribution. Although there are many discrete distributions we have made use of five Discrete Distributions namely, Uniform, Binomial, Poisson, Geometric and Hypergeometric Distributions. software applications, such as MATLAB®, use algorithms that make results appear to be random and independent. However the results are not random in a strict mathematical sense but they pass various statistical tests of randomness and independence. These random numbers are often described as *pseudorandom* and *pseudo-independent*. One advantage of using pseudorandom numbers is that they can be repeated a random number calculation at any time, which is very important in testing and diagnostic situations.

Pseudorandom numbers in matlab are been generated by using one or more random number streams. Some of the functions used are rand, randn or randi. These functions all rely on the same stream of uniform random numbers, known as the *global stream*.

#### RandStream constructor

The RandomStream Constructor is used to create a random number stream that uses the uniform pseudorandom number generator algorithm specified by genotype. The genotype includes Mersenne twister, Multiplicative congruential generator, Multiplicative lagged Fibonacci generator, Combined multiple recursive

generator, Shift-register generator summed with linear congruential generator and Modified subtract with borrow generator. In this paper we have used Multiplicative congruential generator type for the random stream constructor. Transformation Algorithm used by randn to generate normal pseudorandom values includes either 'Ziggurat', 'Polar', or 'Inversion'. In this paper we have made use of Ziggurat Algorithm.

**IV. SCALING OF PSEUDO RANDOM NUMBERS OF DISCRETE DISTRIBUTION**

The Pseudo Random numbers obtained from Discrete Distributions may not be in the range of 0 to 255. As we have to deal with images, the scaling of these pseudo random numbers was important to us. The scaling of the pseudo random numbers were done by the following procedure.

Consider x-axis as the input(for e.g. random numbers obtained by using a discrete distribution between 90 and 180). To scale these numbers between 1 and 256, we can plot a straight line as shown in the figure below. The y-axis represents the output. Considering both the points(x1,y1) and (x2,y2), for e.g. (90,1) and (180,256). Using these two data points and solving them simultaneously we can obtain value of  $m = 255/90$  and  $c = -254$ . Using these two values and input values we can get all the output values which will be scaled between 1 and 256. The scaling method is depicted in the following figure no 6.

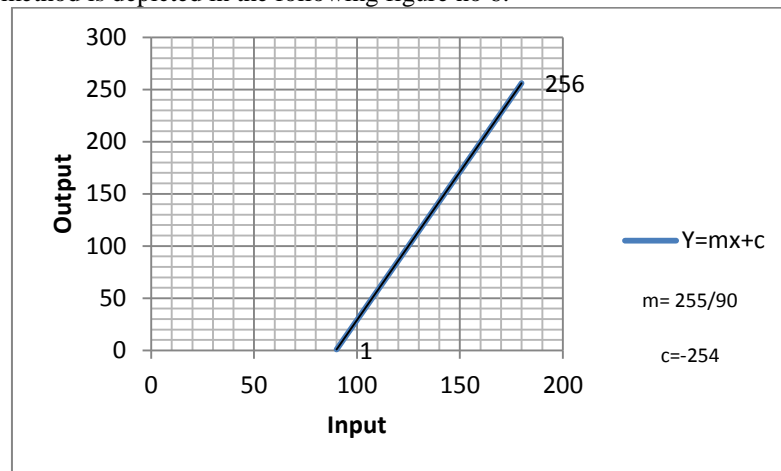


Figure 6. Scaling Method

**V. MOD OPERATOR AND ITS USE FOR IMAGE ENCRYPTION**

The MOD operator in computer language simply means the remainder. For e.g.  $17 \text{ mod } 3 = 2$ . For image encryption we have extended this concept. Let us look at the procedure applied for encryption and decryption.

Let us consider two values  $A = 100$ (original Value)  $B = 200$ (pseudorandom value generated from one of the discrete distributions)

$$C = (A+B) \text{ mod } 256 \tag{12}$$

The result of the above operation results in 44. This result is used as encrypted value.

For decryption

$$A = (C-B) \text{ mod } 256 \tag{13}$$

The above operation results in 100(which is the original value).

**VI. PROPOSED APPROACH**

In this paper, we have made use of pseudorandom numbers generated by the discrete distributions for Image encryption. As described above, using matlab software and customizing the randomstream constructor to specific parameters we set the default stream. The purpose behind doing this, we are trying to study the pseudorandom nature of discrete distributions for Image encryption. We have used MOD as a invertible operator for encrypting the images. The step by step Procedure is given below

**Encryption**

- 1) Read the 24-bit color image
- 2) Generate the Pseudo Random Matrix (size same as the original image) from the desired discrete distribution.



- 3) Use one to one mapping between the Pseudo Random Matrix and the original image and apply the MOD operation as explained above.
- 4) Apply step no 3 to R Plane, G Plane and B Plane Separately.
- 5) Repeat the step no 3 till an encrypted image is formed.
- 6) Save the image obtained in step 4 as Encrypted Color image.

**Decryption**

- 1) Read the 24-bit color Encrypted Image
- 2) Generate the Pseudo Random Matrix (size same as the original image) from the desired discrete distribution.
- 3) Use one to one mapping between the Pseudo Random Matrix and the encrypted image and apply the MOD inverse operation as explained above.
- 4) Apply step no 3 to Encrypted R Plane, Encrypted G Plane and Encrypted B Plane Separately.
- 5) Repeat the step no 3 till original image is obtained.
- 6) Save the image obtained in step 4 as Original image.

**VII. EXPERIMENTAL RESULTS**

For Experimental purpose , we have used 24-bit color images. The proposed approach was tested on five different images of size 256x256. For experimental analysis , different moments like mean , std deviation, skewness and kurtosis of the encrypted image was calculated, a new experimental parameter was also introduced called as Peak Average Fractional Change in Pixel Value(PAFCPV) given in equation 14 below.

$$PAFCPV = \sum_{i=1}^M \sum_{j=1}^N \frac{abs(O(x,y) - E(x,y))}{255} \tag{14}$$

Figure 7.1 shows the 24 bit Color original Image, and its corresponding Histograms of Red , Green and Blue plane are shown in Figure 7.2(a-c).



Figure 7.1 Original Image

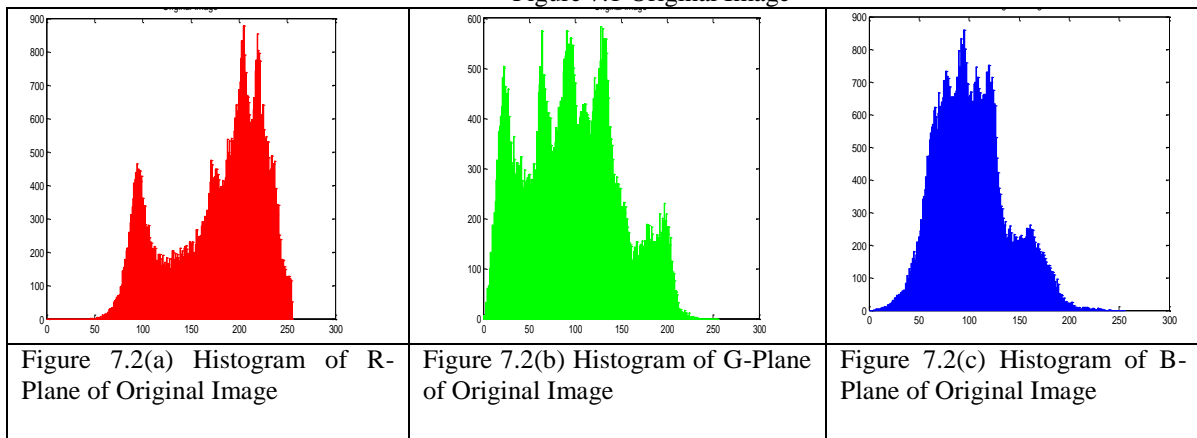


Figure 8.1 shows the encrypted image obtained from Random numbers generated using uniform distribution. The Encrypted image Histogram analysis for Red, Green and Blue planes are shown in Figure 8.2(a-c). Similarly Figure 9.1 shows the encrypted image obtained from Random numbers generated using binomial distribution. The Encrypted image Histogram analysis for Red, Green and Blue planes are shown in Figure 9.2(a-c). Figure 10.1 shows the encrypted image obtained from Random numbers generated using Poisson distribution. The Encrypted image Histogram analysis for Red, Green and Blue planes are shown in Figure 10.2(a-c). Figure 11.1 shows the encrypted image obtained from Random numbers generated using Geometric distribution. The Encrypted image Histogram analysis for Red, Green and Blue planes are shown in Figure 11.2(a-c). Figure 12.1 shows the encrypted image obtained from Random numbers generated using

hypergeometric distribution. The Encrypted image Histogram analysis for Red, Green and Blue planes are shown in Figure 12.2(a-c).

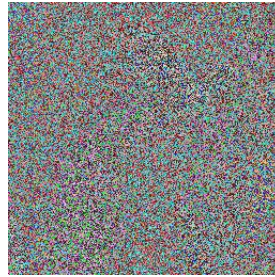


Figure 8.1 Encrypted Image Using Uniform Distribution

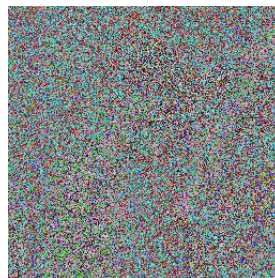
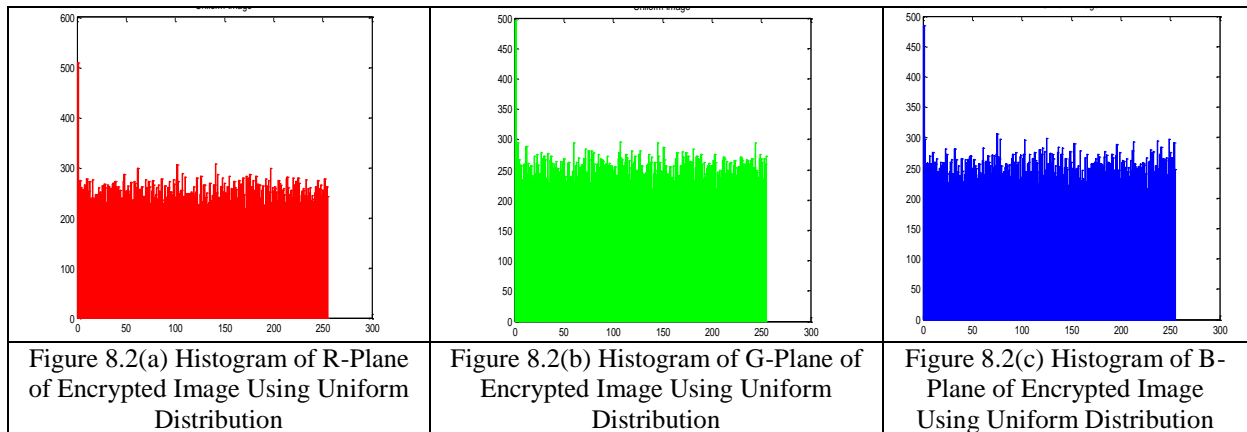
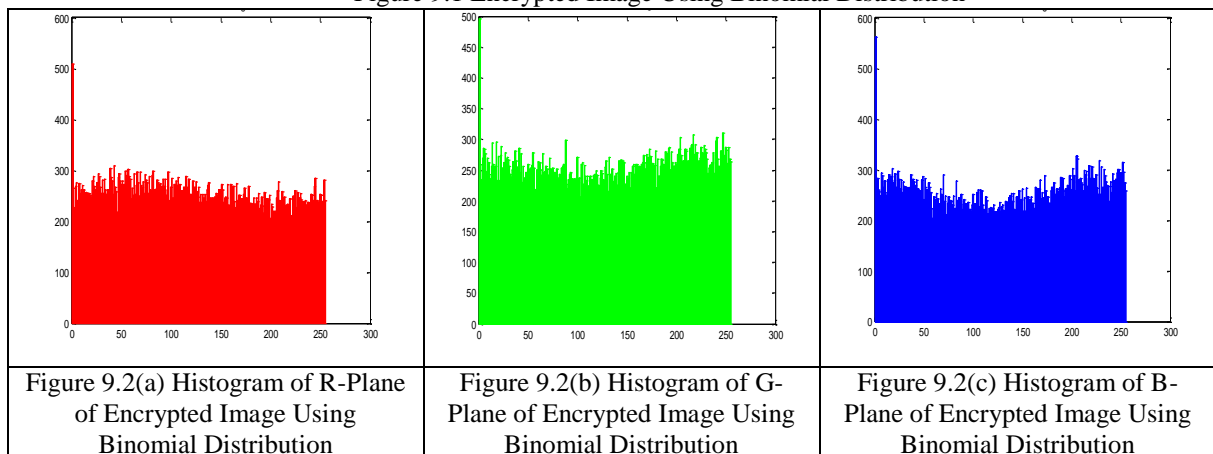


Figure 9.1 Encrypted Image Using Binomial Distribution



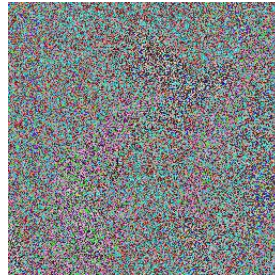


Figure 10.1 Encrypted Image Using Poisson Distribution

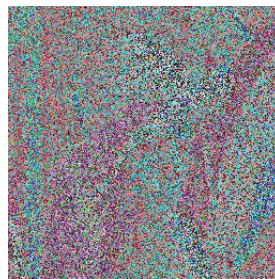
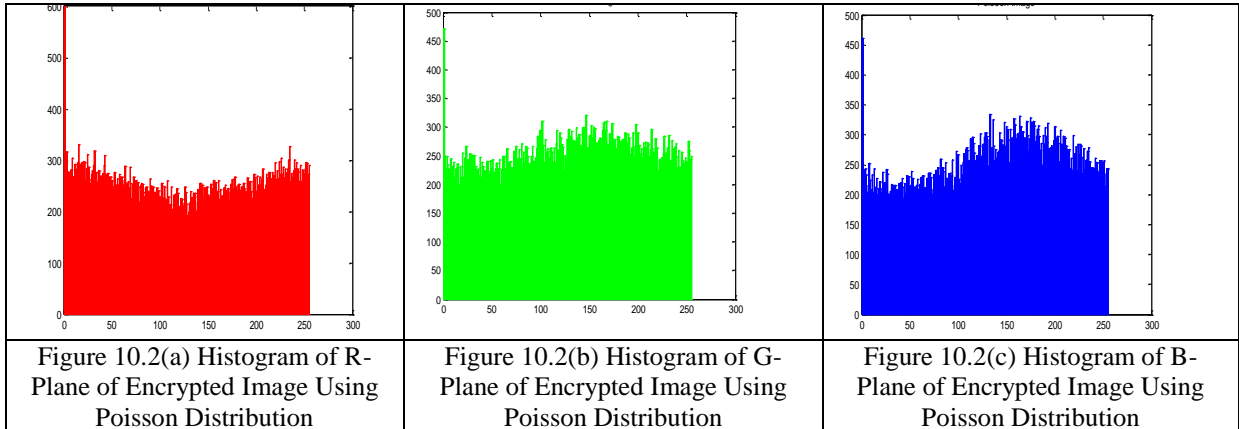


Figure 11.1 Encrypted Image Using Geometric Distribution

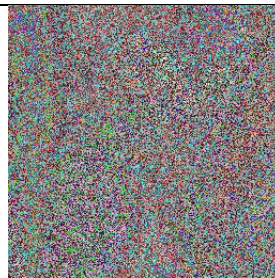
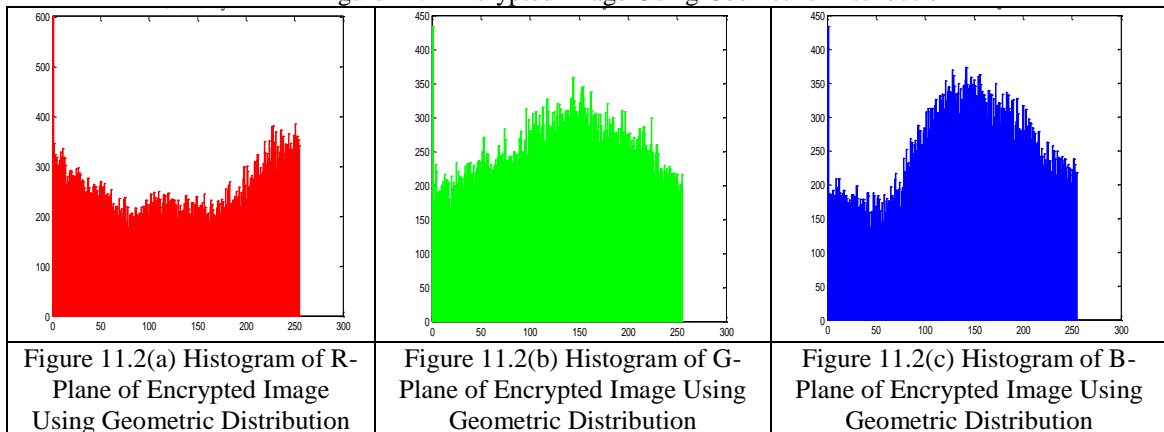


Figure 12.1 Encrypted Image Using Hypergeometric Distribution

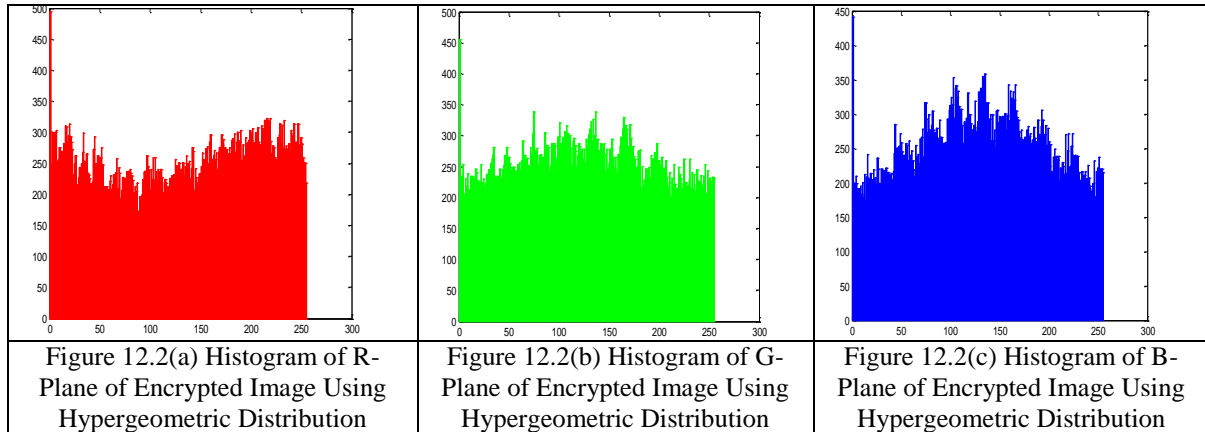


Table No 1. No of Iterations for Discrete Distributions

Discrete Distribution	No of Iterations	Key Combination	
		Uniform	3
Binomial	3	N=256 and Prob=0.5	
Poisson	3	Sample Mean Lambda=128	
Geometric	8	Prob=0.08	
Hypergeometric	3	Total No of Samples 500,Desired type 50,Samples 100	

Table No 1 shows the number of iterations needed for various discrete distributions for encrypting the digital image. From the Table it is observed that Geometric distribution needs the largest number of iterations as compared with other distributions, which require only 3. The Key combination column gives the details on the key space used for each of the distribution, however the key space is not limited to the values stated above. These are the initialization parameter for each distribution along with generator type, random algorithm used and scaling function.

Table No 2. Experimental values obtained for Image Moments like Mean, Std, Skewness, Kurtosis and PAFCPV for Original image, Uniform, Binomial, Poisson, Geometric and Hypergeometric Distributions in Lena Image

Lena		Original	Uniform	Binomial	Poisson	Geometric	Hyper geometric
		MEAN	R Plane	177.17	127.14	124.68	126.95
	GPlane	96.6	127.09	130.76	130.86	131.37	126.91
	BPlane	102.71	127.22	132	133.69	136.52	128.72
STD DEVIATION	R Plane	48.47	73.8	74.92	76.47	78.97	75.63
	GPlane	50.99	73.99	74.28	72.33	69.64	71.09
	BPlane	35.3	74.01	75.04	71.65	67.74	69.25
SKEWNESS	R Plane	-54.25	-80.54	81.6	82.84	-85.20	-82.17
	GPlane	57.55	80.72	-80.97	-79.33	-76.88	78.20
	BPlane	41.08	80.72	-81.67	-78.83	-75.65	-76.51
KURTOSIS	R Plane	58.88	85.51	86.53	87.52	89.73	87.00
	GPlane	62.7	85.67	85.92	84.51	82.28	83.47
	BPlane	46	85.67	86.57	84.18	81.63	81.93
PAFCPV		0	0.303	0.322	0.308	0.293	0.281

From Table No 2, The Image moments are calculated for Red , Green and Blue Plane of the Original and Encrypted Images obtained for various Discrete Distributions. It is observed that all the five distributions encrypted images result in decrease in the mean value in R Plane as compared to original Image R Plane, an increase is observed in mean value of G and B Plane of different distributions. A increase in the std deviation, skewness and kurtosis when compared to original image. PAFCPV is less in Geometric and Hypergeometric Encrypted images as compared to Uniform, Binomial and Poisson Distributions.

Table No 3. Experimental values obtained for Image Moments like Mean, Std, Skewness, Kurtosis and PAFCPV for Original image, Uniform, Binomial, Poisson, Geometric and Hypergeometric Distributions in Minni Image

Minni		Original	Uniform	Binomial	Poisson	Geometric	Hypergeometric
MEAN	R Plane	205.12	127.79	122.73	117.67	104.33	118.94
	GPlane	191.81	127.82	123.32	118.58	106.12	119.14
	BPlane	180.21	127.70	123.36	118.37	104.43	118.33
STD DEVIATION	R Plane	87.79	73.69	70.64	73.20	73.38	77.60
	GPlane	94.02	73.68	70.88	73.15	73.16	77.05
	BPlane	102.99	73.69	70.52	72.64	71.70	76.76
SKEWNESS	R Plane	-107.52	-80.48	77.82	80.34	81.27	83.82
	GPlane	-108.33	-80.47	78.00	80.22	80.72	83.30
	BPlane	-112.77	-80.48	77.69	79.78	79.51	83.11
KURTOSIS	R Plane	123.18	85.49	83.15	85.69	87.61	88.38
	GPlane	120.32	85.47	83.28	85.51	86.74	87.87
	BPlane	121.36	85.48	83.02	85.13	85.79	87.77
PAFCPV			0.454	0.474	0.482	0.510	0.476

From Table No 3, It is observed that all the five distributions encrypted images result in decrease in the mean value compared to original Image, decrease in the std deviation, skewness and kurtosis when compared to original image. PAFCPV is maximum in Geometric as compared to Uniform, Binomial and Poisson Distributions and Hypergeometric.

Table No 4. Experimental values obtained for Image Moments like Mean, Std, Skewness, Kurtosis and PAFCPV for Original image, Uniform, Binomial, Poisson, Geometric and Hypergeometric Distributions in Fruits Image

Fruits		Original	Uniform	Binomial	Poisson	Geometric	Hypergeometric
MEAN	R Plane	153.05	127.19	125.94	128.08	129.58	130.08
	GPlane	93.64	127.33	128.45	128.57	127.67	126.76
	BPlane	28.66	127.83	128.47	121.33	109.62	118.70
STD DEVIATION	R Plane	66.87	73.94	74.47	75.22	76.20	74.44
	GPlane	64.57	73.94	73.96	72.99	71.85	73.01
	BPlane	30.96	73.84	70.63	70.54	67.25	74.49
SKEWNESS	R Plane	-75.14	80.63	81.12	-81.75	-82.71	-81.12
	GPlane	70.59	-80.66	-80.70	-79.82	-78.59	79.89
	BPlane	40.02	-80.60	-77.80	77.81	74.83	81.48
KURTOSIS	R Plane	81.67	85.58	86.02	86.56	87.48	86.05
	GPlane	75.77	85.61	85.67	84.86	83.62	84.95
	BPlane	49.49	85.58	83.13	83.26	80.81	86.68
PAFCPV			0.359	0.371	0.350	0.322	0.332

From Table No 4, Mean in R-Plane decreases in all the five distributions as compared to original image, B-Plane and G-Plane mean increases as compared original image. Std deviation, skewness and kurtosis increases in R,G and B-Plane in all the five distributions. The highest PAFCPV is obtained in Binomial distribution as compared to other distributions

Table No 5. Experimental values obtained for Image Moments like Mean, Std, Skewness, Kurtosis and PAFCPV for Original image, Uniform, Binomial, Poisson, Geometric and Hypergeometric Distributions in RainbowBirds Image

Rainbow Birds		Original	Uniform	Binomial	Poisson	Geometric	Hyper geometric
MEAN	R Plane	168.68	127.18	124.9	125.61	127.37	128.93
	GPlane	157.79	127.51	125.56	126.43	128.52	129.45
	BPlane	124.09	127.78	125.18	124.22	123.76	126.15
STD DEVIATION	R Plane	66.68	73.80	73.76	75.55	78.25	75.88
	GPlane	68.25	74.04	73.99	75.32	77.59	75.41
	BPlane	84.43	73.92	73.05	74.68	76.31	75.94
SKEWNESS	R Plane	- 76.44	80.54	80.56	82.04	84.52	-82.30
	GPlane	-77.08	80.78	80.71	81.83	- 83.94	-81.89
	BPlane	- 89.35	- 80.67	79.90	81.34	82.69	82.36
KURTOSIS	R Plane	85.22	85.50	85.57	86.83	89.09	87.01
	GPlane	84.82	85.74	85.67	86.64	88.57	86.66
	BPlane	93.12	85.64	84.96	86.25	87.37	87.08
PAFCPV			0.348	0.366	0.356	0.344	0.333

From Table No 5, Mean in R and G Plane decreases, there is a increase in B plane mean except for decrease in geometric distribution. Std Deviation increases in R Plane and G plane. In B-Plane std deviation decreases. There is a increase in skewness in the R plane and G plane all the distributions. Skewness decreases in Bplane in all the distributions. Kurtosis increases in R-plane and G-Plane in all the distributions. In B-plane for all the distributions Kurtosis is decreasing. PAFCPV is largest in Binomial Distribution encrypted image.

Table No 6. Experimental values obtained for Image Moments like Mean, Std, Skewness, Kurtosis and PAFCPV for Original image, Uniform, Binomial, Poisson, Geometric and Hypergeometric Distributions in Tiger Image

Tiger		Original	Uniform	Binomial	Poisson	Geometric	Hyper geometric
MEAN	R Plane	102.35	127.71	126.63	123.06	117.15	123.42
	GPlane	108.02	127.42	129.70	130.26	130.34	127.40
	BPlane	54.39	127.80	127.17	123.08	113.95	122.46
STD DEVIATION	R Plane	90.94	73.81	72.14	73.05	72.73	75.36
	GPlane	60.44	74.04	74.16	72.77	71.00	71.79
	BPlane	66.04	73.82	71.76	72.11	70.65	74.79
SKEWNESS	R Plane	96.90	-80.57	79.14	79.96	79.70	81.92
	GPlane	69.02	80.75	-80.86	- 79.67	- 78.20	78.78
	BPlane	78.71	- 80.58	-78.77	79.14	77.66	81.44
KURTOSIS	R Plane	101.89	85.56	84.31	85.07	84.97	86.75
	GPlane	76.00	85.69	85.81	84.77	83.54	83.95
	BPlane	90.68	85.56	83.95	84.35	83.03	86.33
PAFCPV			0.367	0.377	0.358	0.328	0.341



From Table No 6, there is a increase in mean across all the three planes and all the distributions. Std deviation is decreasing in R-Plane in all the distributions, G-plane and B-plane the std deviation is increasing across all the distributions. Skewness is decreasing in all the distributions in the R-plane, In G-plane skewness is increasing in all the distributions, in B-plane there is a decrease in skewness only in geometric distribution. Kurtosis is decreasing in R and B plane, It is seen that Kurtosis is increasing in G-plane. PAFCPV is highest in Binomial Distribution.

### VIII. CONCLUSION

The proposed approach was applied on 24-bit color images. The three planes R, G and B planes were encrypted using the proposed approach. This approach uses randomness of different discrete distributions, like Uniform, Binomial, Poisson, Geometric and Hypergeometric for image encryption. All the five distribution gives a good histogram analysis for encrypted images which can be seen from the results displayed above. For experimental analysis, Image Moments were studied for all the encrypted images obtained by applying different distributions. From the results obtained it is clear that, irrespective of the image the statistical moments show very small variation. With the change of original distribution these moments take a different value and display the same property. The PAFCPV parameter whose range is between 0 to 1 is used for measuring the peak average fractional change in pixel value of encrypted image. For an Encrypted image an ideal case should have a value of 1, In this proposed approach we have obtained a maximum value of 0.5 for Minni image for PAFCPV.

### REFERENCES

- [1] Mishra, Minati, Priyadarsini Mishra, M. C. Adhikary, and Sunit Kumar. Image Encryption Using Fibonacci-Lucas Transformation, *International Journal on Cryptography and Information Security (IJCIS)*,2(.3), September 2012, 131-141.
- [2] Zhu, Guiliang, Weiping Wang, Xiaoqiang Zhang, and Mengmeng Wang. Digital image encryption algorithm based on pixels, *Proc. IEEE Conf. on Intelligent Computing and Intelligent Systems (ICIS)*, (1), 2010 , 769-772.
- [3] Feng, Yong, and Xinghuo Yu. A novel symmetric image encryption approach based on an invertible two-dimensional map, *Proc. 35th IEEE Conf. on Industrial Electronics, IECON'09. 2009*, 1973-1978.
- [4] Pawan N. Khade and Prof. Manish Narnaware, 3D Chaotic Functions for Image Encryption, *IJCSI International Journal of Computer Science Issues*, 9( 3),(1), May 2012, 323-328.
- [5] Mohammed A. Shreef, Haider K. Hoomod, Image Encryption Using Lagrange-Least Squares Interpolation, *International Journal of Advanced Computer Science and Information Technology (IJACSIT)* 2, (4), 2013, 35-55
- [6] Zhou, Yicong, Sos Agaian, Valencia M. Joyner, and Karen Panetta, Two Fibonacci p-code based image scrambling algorithms, *Proc Conf on Electronic Imaging , International Society for Optics and Photonics*, 2008, 681215-681215.
- [7] Manjunath Prasad and K.L.Sudha, "Chaos Image Encryption using Pixel shuffling" published in D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, 2011, 169-179.
- [8] Sathyanarayana, S. V., M. Aswatha Kumar, and KN Hari Bhat. Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points. *IJ Network Security*, 12(3) ,2011, 137-150.
- [9] Wei-bin, Chen, and Zhang Xin, Image encryption algorithm based on Henon chaotic system, *Proc. IEEE Conf. on Image Analysis and Signal Processing, IASP 2009*, 94-97.
- [10] Younes, Mohammad Ali Bani, and Aman Jantan. Image Encryption Using Block-Based Transformation Algorithm, *International Journal of Computer Science IAENG*, 35( 1), (2008)
- [11] Shah, Jolly, and Vikas Saxena. "Performance Study on Image Encryption Schemes." *International Journal of Computer Science Issues (IJCSI)* 8, ( 4)( 1), 2011, 349-355
- [12] Rathod, Hiral, Mahendra Singh Sisodia, and Sanjay Kumar Sharma., Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm), *International Journal of Computer Technology and Electronics Engineering (IJCTEE)* 1 (3), 2011, 7-13.
- [13] Sun, Yuanyuan, Lina Chen, Rudan Xu, and Ruiqing Kong. "An Image Encryption Algorithm Utilizing Julia Sets and Hilbert Curves." *PloS one* 9(1) (2014)
- [14] Ahmad, Jawad, and Fawad Ahmed. Efficiency Analysis and Security Evaluation of Image Encryption Schemes, *International Journal of Video & Image Processing & Network Security* 12(4), 2012.18-31