ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

# Image Encryption And Compression Using Prediction Error K-Mean Clustering And Cyclic Permutation

**Praveen Kumar**[1]
Assistant Professor CSE Dept
CERT Meerut, India

**Maitreyee Dutta**[2]
Ph.D
Professor & Head, CSE Dept.
NITTTR, Chandigarh. India

***Abstract:*** ***In most of applications, encryption of an image is done prior image compression. This create problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be effectively performed. In this paper the Author will design a good image encryption-and-compression technique, where lossless and lossy compression is taken into consideration. The suggested image encryption technique is operated in prediction error domain and k-mean clustering with cyclic permutation, this technique is able to provide a reasonably more security. We show that an arithmetic coding-based method can be implemented to efficiently compress the encrypted images. More clearly, the proposed compression method which is applied to encrypted images will be effective in the form of compression efficiency, than the lossless and lossy image encoders, which take actual images as inputs.***

***Keywords- K-Mean Clustering, Cyclic Permutation,, Prediction Error, GAP, PSNR ,BPP (Bit Per Pixel).***

## I. INTRODUCTION

The major challenge in Encryption-and-Compression system is that compression has to be conducted in the encrypted domain, In the following figure A wants to securily and effectively transmit an image I to a receipient C through a unsecure chhanel provider B.The system of Encryption and Compression system is illustrated in Figure. 1

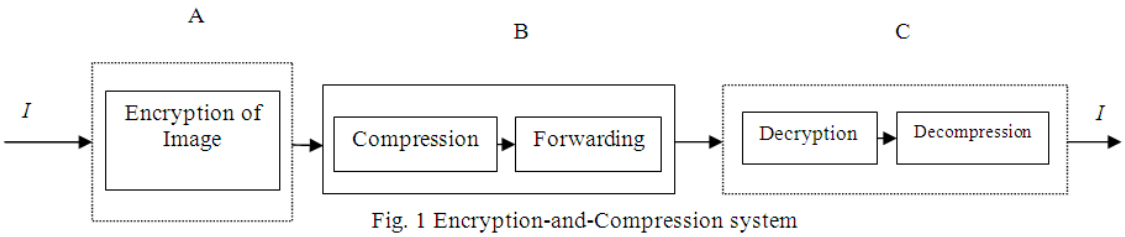



Fig. 1 Encryption-and-Compression system

The processing of encrypted images directly in the encrypted domain has been become more popular[1]-[5] now days First of all it become not feasible for B to compress the encrypted data, since no image structure can be create to enable a conventional compressor. However the stream cipher encrypted data is compressible with the use of coding with external information principles, without compromising either the compression efficiency or security. In addition to the theoretical findings also proposed practical algorithms to losslessly compress the encrypted binary images.

## II. PREDICTIOIN ERROR

Prediction error (PE) measures how well the model is able predict the outcome for new observations not used in developing the prediction model.

### *a) Measures of Prediction Error*

For each pixel $I_{p,q}$ of the image I to be encrypted, a prediction $I'_{p,q}$ is first made by using an image predictor, e.g. GAP [6] , according to its causal surroundings. In our work, the GAP is used because its de-correlation capability is excellent. Each prediction error $I'_{p,q}$ .is reshape in $I''_{p,q}$ by using a feedback process. Then we calculate the prediction error associated with $I_{p,q}$ as follows..

$$E_{p,q} = I_{p,q} - I''_{p,q} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad \ldots\ldots\ldots\ldots \quad \ldots\ldots(1)$$

The prediction error $E_{p,q}$ may be any value from [-255,255],that will mapped in a range [0,255] In our proposed method encryption is done in the domain of mapped prediction error $E'_{p,q}$ Although for 8-bit images, the prediction error $E_{p,q}$ can potentially take any values in the range [−255, 255], it can be mapped into the range [0, 255], by considering the fact that the predicted value $\tilde{I}I''_{p,q}$ is available at the decoder side.Our proposed image encryption algorithm is performed over the domain of the mapped prediction error $E'_{p,q}$ Instead of treating all the prediction errors as a whole, we divide the prediction errors into L clusters based on a context-adaptive approach. The subsequent randomization and compression will be shown to be benefited from this clustering operation. To this end, an error energy estimator originally proposed in [7] is used as an indicator of the image local activities. More specifically, for each pixel location (p,q ), the error energy estimator is defined by

$$Diff(p,q) = d_1 + d_2 + 2(abs(E_{p-1,q})) \quad (2)$$

where

$$d_1 = abs(I_{p-1,q} - I_{p-2,q}) + abs(I_{p,q-1} - I_{p,q-1}) + abs(I_{p,q-1} - I_{p+1,q-1})$$

$$d_2 = abs(I_{p-1,q} - I_{p-1,q-1}) + abs(I_{p,q-1} - I_{p,q-2}) + abs(I_{p+1,q-1} - I_{p+1,q-2}) \quad (3)$$

and $E_{p-1,q}$ is the prediction error at location (p − 1, q ).

## III. IMAGE ENCRYPTION USING PREDICTION ERROR K-MEAN CLUSTERING AN CYCLIC PERMUTATION

The complete process of encryption of an image is shown in the following figure 2

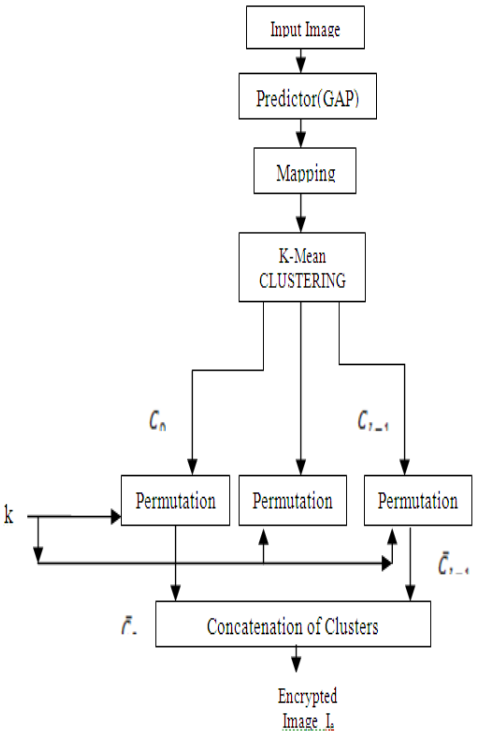



*Fig. 2 Diagram of image encryption*

## IV. K-MEAN CLUSTERING

K-mean clustering alogorithm contains the following steps:

1. First choose randomly k centroids from the set of data for desired number of clusters

2. Assigning every data object to the cluster with the nearest centroid

3. Update the centroids by computing the mean values of objects in the clusters

4. Repeat step 1 ,2 and 3 untill termination criteria not found

## V. ENCRYPTION ALGORITHM

The algorithmic procedure of performing the image encryption is then given as follows:

**Step 1:** Calculate all the prediction errors $E^{I}_{p,q}$ of the image I .

**Step 2:** Splitting all the prediction errors into L no of clusters i.e. $\mathbf{C}_k$ for $0 \le k \le L-1$, where each $\mathbf{C}_k$ is build by concatenating the mapped prediction errors in the raster-scan manner.

**Step 3:** Resizing the prediction errors in every $\mathbf{C}_k$ into a two dimensional block which have four columns and abs($\mathbf{C}_k$ )/4 rows.

**Step 4:** Applying cyclic shift operations to each output of prediction error block, and read the data in raster-scan manner to obtain the permuted cluster $C_k$ .

**Step 5:** The assembler concatenates all the permuted clusters $C_k$ for $0 \le k \le L-1$, and generates the final output encrypted image

$$I_e = C^{I}_0 \; C^{I}_1 \ldots\ldots\ldots\ldots C^{I}_{L-1} \qquad (4)$$

where size of each prediction error is 8 bits.

**Step 6:** Provide $I_e$ to B, along with the length of each cluster abs($C^{I}_k$) for $0 \le k \le L-2$.Where B divide Ie into L

No of clusters correctly.

## VI. LOSSLESS COMPRESSION OF ENCRYPTED IMAGE BY ADAPTIVE ARITHMETIC CODING

Following figure shows the compression of encrypted image Ie with side information abs($C^{I}_k$) for 0<=k<=L-2, A de-assembler can be used to divide Ie in L segments $C^{I}_0$ $C^{I}_1$ ..... $C^{I}_{L-1}$ .An adaptive arithmetic coding is applied to lossless coding each prediction error sequence $C^{I}_k$ into a bit stream $S_k$ in parallel manner to increase the throughput

$$S=S_oS_1S_2\ldots\ldots\ldots\ldots S_{L-1}$$

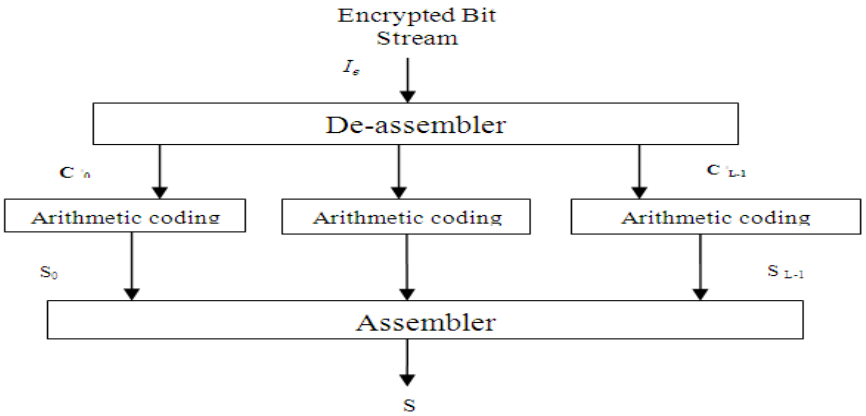



*Fig.3 Lossless Compression by Arithmetic Coding*

## VII. Security And Performance Analysis

If the attacker implement any attacking scheme of directly decoding the encrypted image. of figure 4 which are ten images of size 512 × 5125, the PSNR results are shown in figure 5 of the reconstructed images, where x-axis shows the image number and y axis shows PSNR .We can see that all the PSNR values are near about 9.5 dB, which is very low to convey any useful meaning full information .therefore this system is more secure than other systems

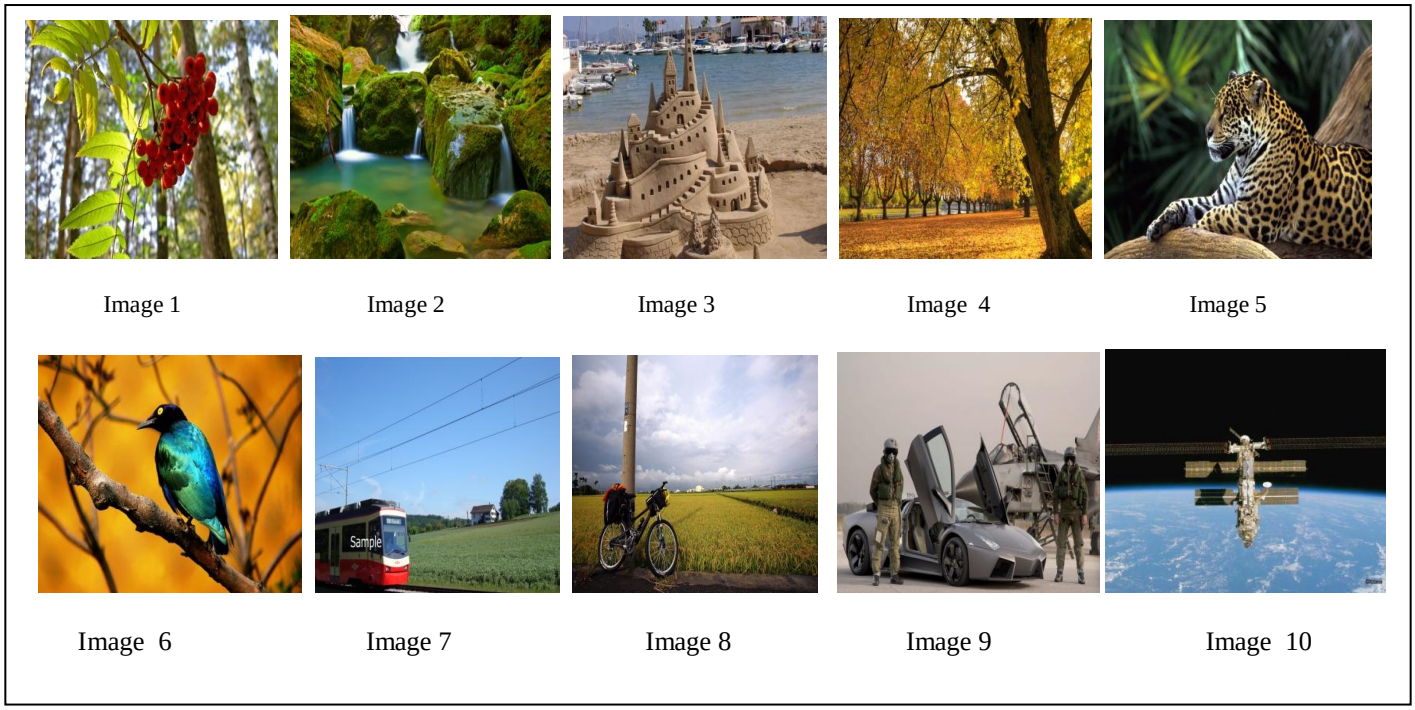



*Fig.4 Test set images*

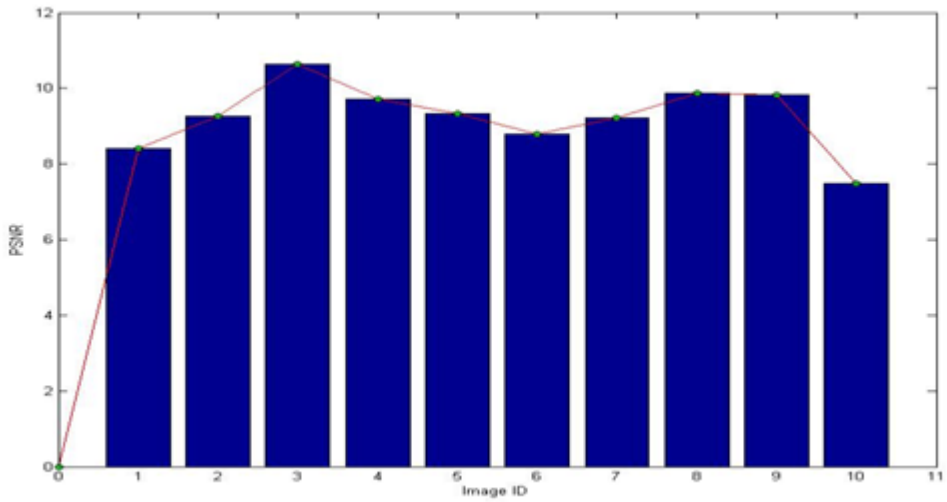



*Fig.5 Results of direct decoding compressed and encrypted image*

**TABLE I**

**Comparison of Lossless Compression Performance**

| Image | Proposed Method | CALIC Method | [10] Method | Saving bits over CALIC(Sc) | Saving bits over 10($S_{[10]}$) |
|---|---|---|---|---|---|
| **Image1** | 134200 B (4.095bpp) | 134232 B (4.096 bpp) | 4.918 bpp | 0.24% | 16.73% |
| **Image2** | 133858 B(4.085 bpp) | 143974 B(4.394 bpp) | 5.271 bpp | 7.03% | 22.50% |
| **Image3** | 120580 B(3.679 bpp) | 150850 B(4.604 bpp) | 5.453 bpp | 20.09% | 32.53% |
| **Image4** | 134165 B(4.094 bpp) | 134651 B(4.109 bpp) | 5.374 bpp | 0.36% | 23.81% |
| **Image5** | 152136 B(4.642bpp) | 142361 B(4.345bpp) | 5.424 bpp | -6.42% | 14.41% |
| **Image6** | 140584 B(4.290 bpp) | 160487 B(4.898 bpp) | 6.206 bpp | 12.41% | 30.87% |
| **Image7** | 111256 B(3.395 bpp) | 121172 B(3.698 bpp) | 5.045bpp | 8.19% | 32.70% |
| **Image8** | 142987 B(4.363 bpp) | 150223 B(4.584 bpp) | 6.124 bpp | 4.82% | 28.75% |
| **Image9** | 157503 B(4.806 bpp) | 177252 B(5.409 bpp) | 6.303 bpp | 11.14% | 23.75% |
| **Image10** | 134623 B(4.108 bpp) | 154264 B(4.708 bpp) | 5.370 bpp | 12.74% | 23.50% |
| **Averaged** | 4.15bpp | 4.449bpp | 5.575bpp | 7.05% | 24.95% |

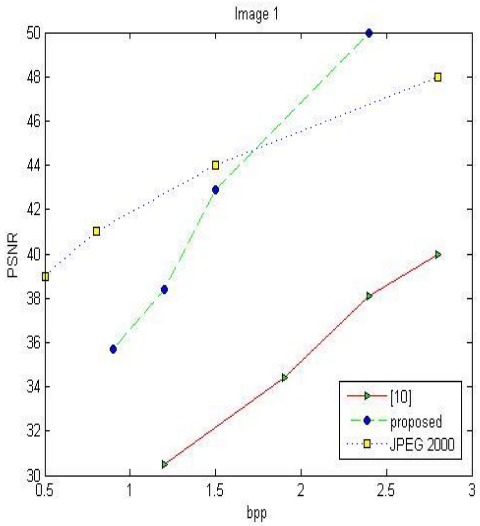
## VIII. RESULT ANALYSIS

Table I, shows that compression efficiency of our proposed method which is applied to the encrypted images is compared with the lossless technique given by the recent version of CALIC[11], which is a good lossless image codecs, and the method in [10], an application lossless compression approach on encrypted images. in Fig. 4 We have taken 10 image samples out of 100 images population which composed various attributes,. Here 'B' stand for bytes and 'bpp' stand for bit per pixel, .

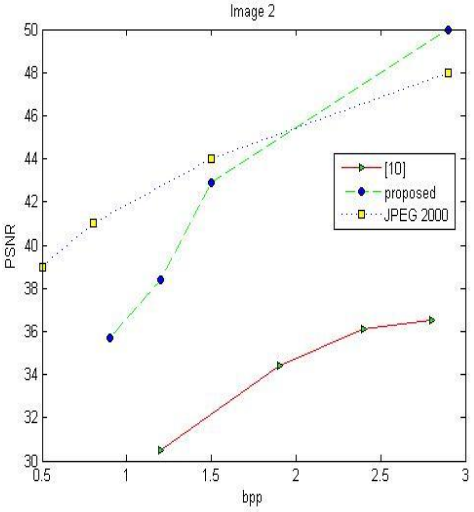
In this table the last two columns which are *Sc* and $S_{[10]}$ stand for the bit rate saving of our proposed method over the CALIC and the method in [10], respectively. The results of this method are obtained by taking the average of 10 random trials.In table I last row gives the averaged results over the 100 images in the test set. It is found that the coding penalty occurred by our method is lower than 0.09% when comparing with the results of the CALIC., the bit rate saving over the method in [10] can be up to 32.*70*%, which is achieved by the image 7.

In Fig. 6 (a to j),the comparison is done in terms of rate-PSNR performance of our proposed method with JPEG 2000 and the method in paper [10]. When the bit rates is more than 2 bpp, then our method achieves large PSNR values than JPEG 2000. The gain in PSNR over JPEG 2000 can be significant for high bit rates. For instance, for image 1, the gain is more than 1.9 dB. As bit rate decrease, the PSNR gain over JPEG 2000 reduces.

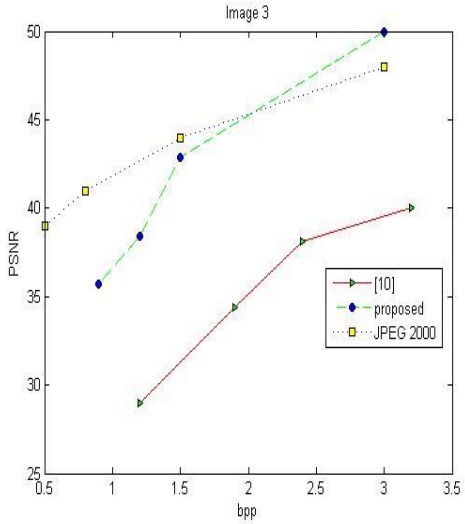
 



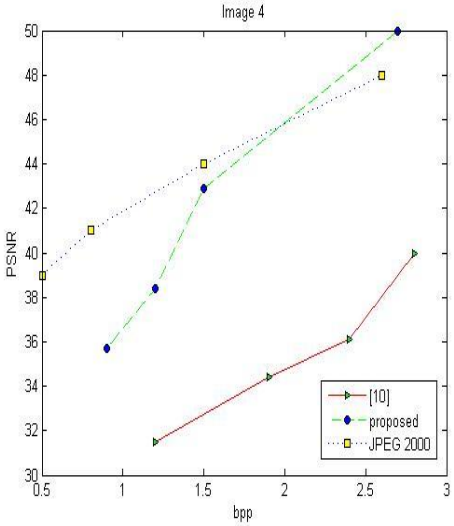

*(a)*



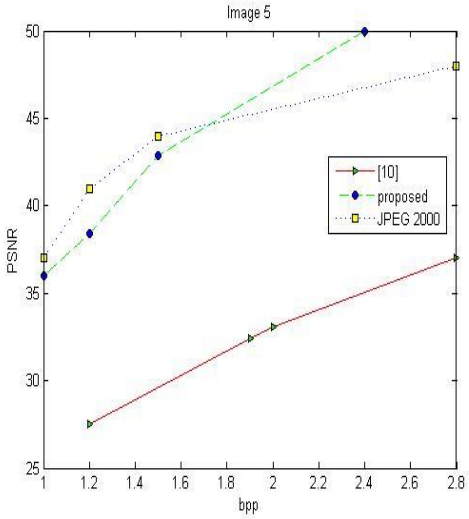

*(b)*



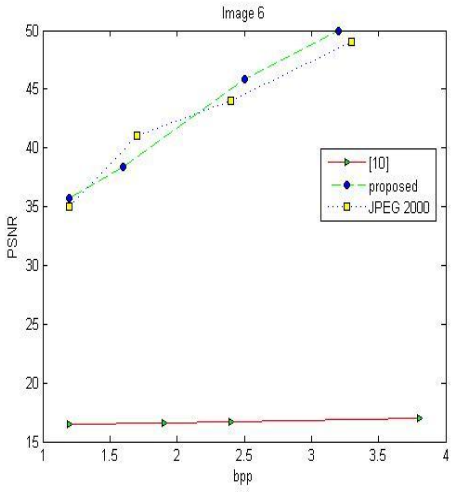

*(C)*




*(D)*

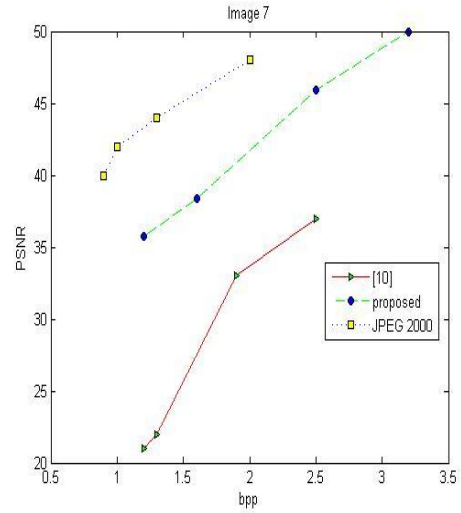



*(E)*

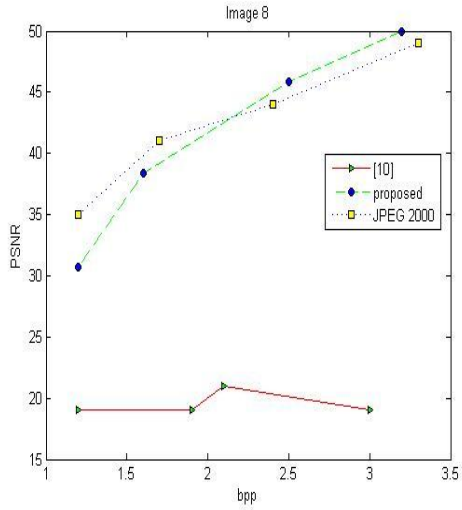



*(F)*

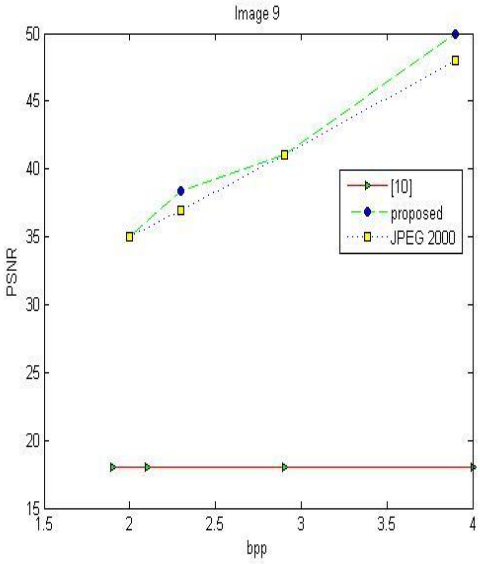
 



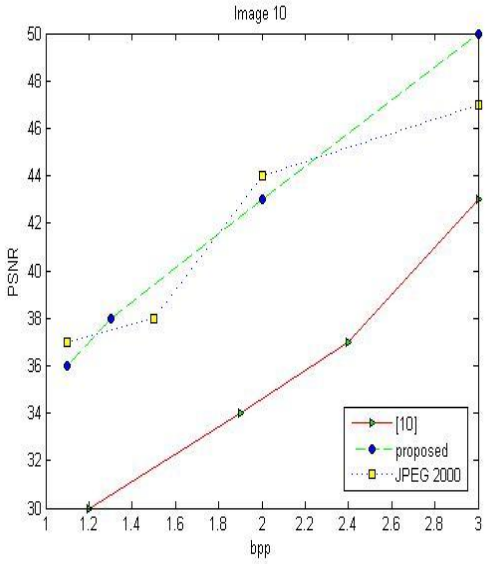

*(G)*




*(H)*




*(I)*




*(J)*

***Fig.6 Comparison of PSNR and bpp of each image***

## IX. CONCLUSION

In our proposed method we have designed an efficient image Encryption-and-Compression system. Within the proposed method, the image encryption is done through prediction error k-mean clustering and cyclic permutation. In this method k-mean clustering is used because it is fast and easier to understand and it also gives best result when data set are distinct or well separated from each other. Good compression of the encrypted image has then been implemented by a context-adaptive arithmetic coding technique The experimental results shows that high level of security has been obtained The coding efficiency of our proposed compression method on encrypted images is very close to lossless and lossy image codecs, which take original, images as inputs.

## References

1. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.
2. T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.

3. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.
4. M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider,"Privacy-preserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 452–468, Jun. 2011.
5. Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1053–1066, Jun. 2012
6. X. Wu and N. Memon, "Context-based, adaptive, lossless image codec," IEEE Trans. Commun., vol. 45, no. 4, pp. 437–444, Apr. 1997.
7. A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760–764.
8. J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption then compression System," in Proc. ICASSP, pp. 2872–2876, 2013.
9. R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey level and color images," in Proc. 16th Eur. Signal Process. Conf., August 2008,
10. W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Imag. Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
11. X. Wu and N. Memon, "Context-based, adaptive, lossless image codec,"IEEE Trans. Commun., vol. 45, no. 4, pp. 437–444, Apr. 1997.
12. A. Kumar and A. Makur, "Distributed source coding based encryptionand lossless compression of gray scale and color images," in Proc.MMSP, 2008, pp. 760–764.

## AUTHOR(S) PROFILE

Praveen Kumar, received the B.Tech. Degree in Information Technology from Bundelkhand Institute of Engineering & Technology, Jhansi, Uttar Pradesh in 2007. Currently pursuing Master's Degree in Computer Science and Engineering from NITTTR Chandigarh (punjab).