Privacy Preserving Haze Removal

Manas Gupta

Ankit Chawla

Applied Mathematics 3rd Year

Under the guidance of -

Dr. Balasubramanian Raman, Associate Professor

Department of Computer Science

IIT Roorkee

Table of Contents

1. INTRODUCTION

Nowadays the visual data in the world is increasing rapidly. With limited storage spaces in personal electronic devices, the usage of cloud storages has bloomed. These images are stored in an encrypted format in the cloud servers to ensure privacy.

A lot of this visual data comprises images that are clicked in an external environment. Due to the presence of particulate matter(dust, smoke, fog) in the atmosphere, the quality of the images gets degraded. The degradation is closely related to a number of factors such as the gap between object and camera, blur resulting from miss-focus associated with a digital camera, relative climatic issues, and some others. Excessive light entering the camera can also lead to degradation of the images. Thus haze removal becomes highly desired for both personal and professional photography [1].

Taking inspiration from the already existing method of zooming and cropping images directly in the encrypted domain, we aimed to find a method in which we could perform haze removal on the images on the cloud servers directly. Thus it shall enable a user to view a haze free image on the cloud itself and download it if needed. This can be useful for both personal uses and for organisations making use of satellite images as they can save their own storage spaces.

Technical Challenges

An early attempt to achieve this goal was to implement the highly secure Shamir Sharing Technique, perform haze removal in the encrypted domain and then decrypt it. This however, resulted in a technical challenge due to the fact that Shamir Secret Sharing involves going into the modular domain. The reader can read more about Shamir Secret Sharing Technique in Section 2.2.1.

The Shamir Sharing Scheme used by us is a (6,3) threshold scheme. Figure 1 shows the results obtained by using this encryption technique and the haze removal method discussed above. As it can be seen in Figure 1(c), the output image formed fails to make sense as removing haze directly from the encrypted images changes pixels values which in turn change the Lagrange Interpolation drastically.

(a) (b) (c)

Figure 1. (a) Original Image. (b) Encrypted Image (c) Image formed after haze removal by our approach.

To handle such technical challenges we tried to implement relatively less secure methods like chaotic maps to accomplish our desired results.

This report comprises of 4 other sections. Section 2 consists of the Literature Review which covers the details of the methods that have been already developed and have been used by us. Section 3 depicts our results after applying the proposed method and covers both the haze removal analysis and the security analysis of the images. Section 4 is the conclusion of our results. Section 5 mentions the references.

The work performed by us was on relatively small sized images. The code was written in python 2.7 making use of the OpenCV(cv2), and NumPy package.

2. LITERATURE REVIEW

2.1 Haze Removal Technique

The Haze Removal technique used has been given in [2] and [3].

A. Haze Removal Model

In computer vision, the model widely used to describe the formation of a hazy image is

$$I(x) = t(x)J(x) + (1 - t(x))\,A \tag{1}$$

where I is the observed intensity, J is the scene radiance, A is the global atmospheric light, and t is the medium transmission describing the portion of the light that is not scattered and reaches the camera.

B. Dark Channel Prior

For an arbitrary image J, its dark channel is given by

$$J^{\text{dark}}(\mathbf{x}) = \min_{\mathbf{y}\in\Omega(\mathbf{x})} \left(\min_{c\in\{r,g,b\}} J^c(\mathbf{y}) \right), \tag{2}$$

Where J^c is a colour channel of J and $\Omega(x)$ is a local patch centred at x. If J is an outdoor haze free image then intensity of J's dark channel tends to zero.

C. Estimating Atmospheric Light and Transmission

For estimating atmospheric light we take top 0.1% pixels of dark channel (most haze opaque pixels) and find the maximum intensity value for those pixels in the input image.

Assuming transmission in a local patch to be constant, it's expression is given by

$$\tilde{t}(\mathbf{x}) = 1 - \omega \min_{\mathbf{y}\in\Omega(\mathbf{x})} \left(\min_{c} \frac{I^c(\mathbf{y})}{A^c} \right). \tag{3}$$

Due to the phenomenon of Aerial perspective, the parameter ω is used to prevent the full elimination of haze, the full elimination of haze would result in an unnatural image and the loss of depth perception.

We have used $\omega = 0.95$ to find the results.

D. Guided Filtering

We have refined the transmission map using the algorithm [4]. In this case the guidance image is the transmission map and it is filtered using the grayscale input image. The algorithm is based upon the mean and co-variance of the mentioned images.

E. Recovering the Scene Radiance

The final scene Radiance *J(x)* is given by

$$J(x) = \frac{I(x) - A}{\max(t(x), t_0)} + A \,. \tag{4}$$

where the typical value of $t_0 = 0.1$.

F. Post Processing

For making the proposed haze-removal method more robust, the post-processing is added for handling the situation that the haze of the input image is non-uniform distribution with insufficient brightness.

We have used the Bilateral filter Local Contrast Correction Method [5] to improve the exposure of the colours in the image.

The output image is given by

$$O(x,y) = 255\left(\frac{J'(x,y)}{255}\right)^{\alpha^{\left(128 - \frac{BFmask(x,y)}{128}\right)}} \tag{5}$$

$$J'_{inv}(x,y) = 255 - J'(x,y) \tag{6}$$

where *BFmask(x,y)* is obtained by bilateral filtering of the inverted image , α is a parameter depending upon the mean intensities of input image and J'_{inv} is the final output image.

2.2 Encryption Techniques

The following encryption techniques were used -

2.2.1 Shamir Secret Sharing Technique

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir [6]. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Mathematical definition -

The goal is to divide secret S into n pieces of data $S_1, \ldots, S_n$ is such a way that -

1. Knowledge of any k or more S_i pieces makes S easy to compute. That is, the complete secret S can be reconstructed from any combination of k pieces of data.

2. Knowledge of any $k-1$ or fewer S_i pieces leaves S completely undetermined, in the sense that the possible values for S seem as likely as with knowledge of 0 pieces. Said another way, the secret S cannot be reconstructed with fewer than k pieces.

The scheme is called (k,n) threshold scheme.

Shamir Secret Sharing on Images -

In the case of images, a single image is divided into n shares or images such that at least k shares or images are required for the reconstruction of the image [7]. These n images are saved at n different data centres that ensures that information cannot be revealed at any one data centre.

The n images are generated by making a $k-1$ dimensional polynomial where the value of the constant is the value of the pixel and the other variables receive a random coefficient. The n shares are generated by substituting n different values to the polynomial to achieve the corresponding pixel value. The original image can later be generated from any k images using of any interpolation technique. In this project we made use of the Lagrange Interpolation technique for that purpose.

The shares are generated using the following polynomial:

$$[x]_i^{m,k} = \sum_{j=1}^{k-1} (\alpha_j t_i^{\,j} + x) \mod m \tag{7}$$

where x is a secret number in a finite field F_m and $[x]_i^{m,k}$ is the i^{th} share where $i = 1, 2, \ldots n$. a_j's are uniformly distributed random numbers in the finite field, m is a large prime number and t_i is a public constant.

Following we have illustrated a case of Shamir Secret Sharing Technique using a (6,3) threshold scheme -

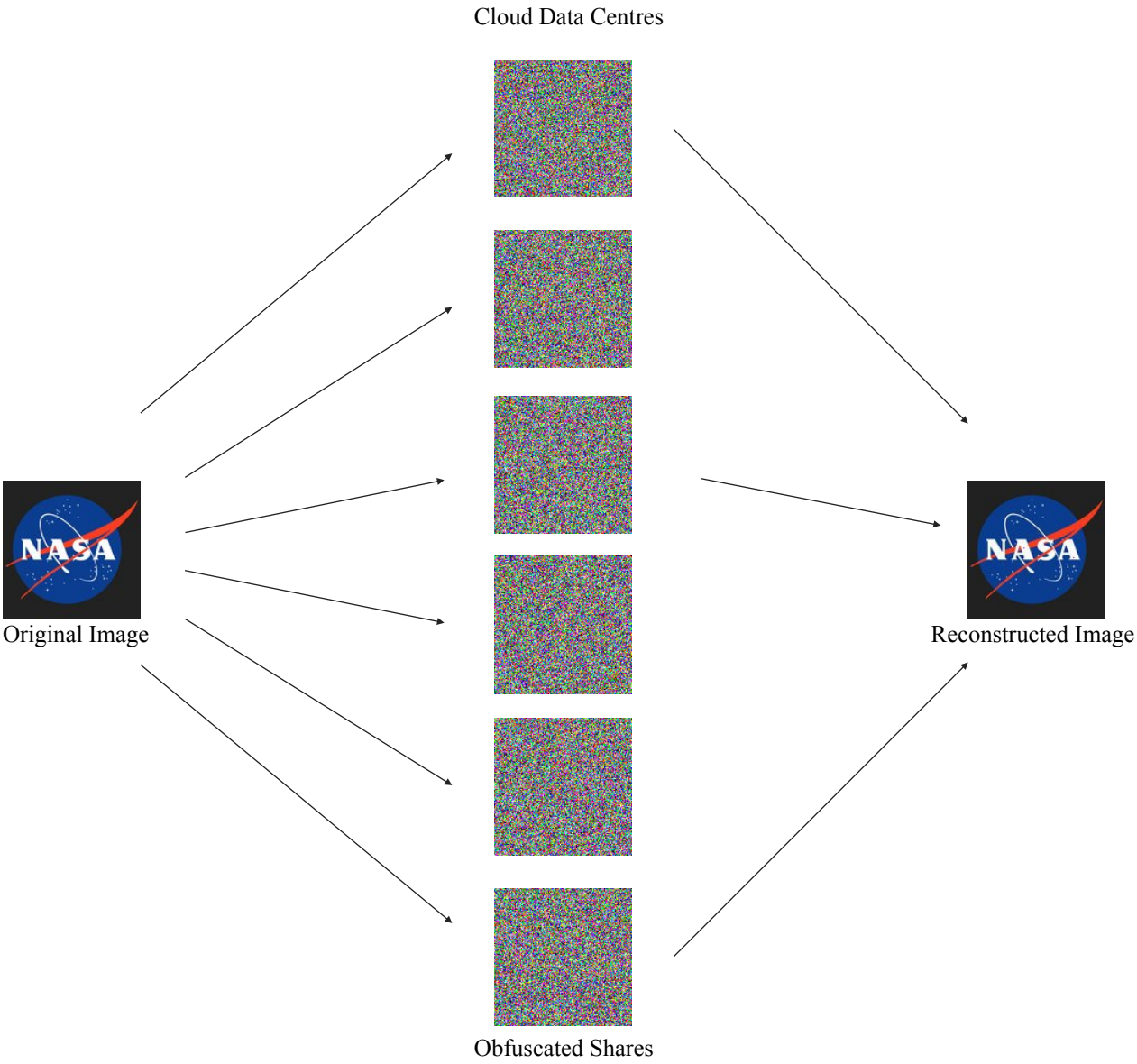


Figure 2. Working of Shamir Sharing Technique

In this the original image is divided into 6 obfuscated shares such that at least 3 are required for the reconstruction. The image is reconstructed by applying Lagrange Interpolation on the 1st, 3rd and the 6th share.

2.2.2 Diffusion and Multiple Chaotic Maps

Chaos theory describes the behaviour of certain nonlinear dynamic system that under specific conditions exhibit dynamics that are sensitive to initial conditions. The two basic properties of chaotic systems are the sensitivity to initial conditions and Mixing Property [8]. Amongst the various types of existing chaotic maps, a self defined chaotic map has been used. The chaotic maps were merged and implemented in different ways to obtain ideal results.

The chaotic map used by us has been defined as -

$$x(n+1) = \{\mu(1 - x(n))\} \tag{8}$$

where *{x}* denotes the fractional part of x as values of x lie in the range [0,1). μ can have values varying from 0 to 4. We have used $\mu = 3.999$ as it helps achieve distinct maps more easily. *x(0)* is chosen randomly between 0 and 1.

These values then have been mapped from [0,1) to 0,1,…,N using the following operation -

$$p(x(n)) = [x(n) * N] \tag{9}$$

where *[x]* denotes the integral part of x and N denotes the total number of pixels we are considering for the chaotic map. For different methods value of N differs. They have been discussed later.

To obtain desired results we have used chaotic maps in different manners -

1. **Row Interchange**

In this we treated each row as a distinct chaotic map. Thus if provided with an $n*m$ image. We created m chaotic maps each having n elements ($N=n$) in them.

2. **Row and Column Interchange**

After performing chaotic maps on row, on the new image we further applied chaotic maps by treating each column as distinct chaotic maps. This time we have n chaotic maps each having m elements.

3. **Box Method**

In this we divide our image into square boxes of some variable dimension x which can vary from image to image. Then the pixels in that box form a chaotic map having $x*x$ elements.

4. Zig-Zag Diffusion

In this the whole images is considered as one big chaotic map and the pixels are numbered in a zig-zag manner which proves to be more effective than taking the elements linearly row/column wise.

3. RESULTS

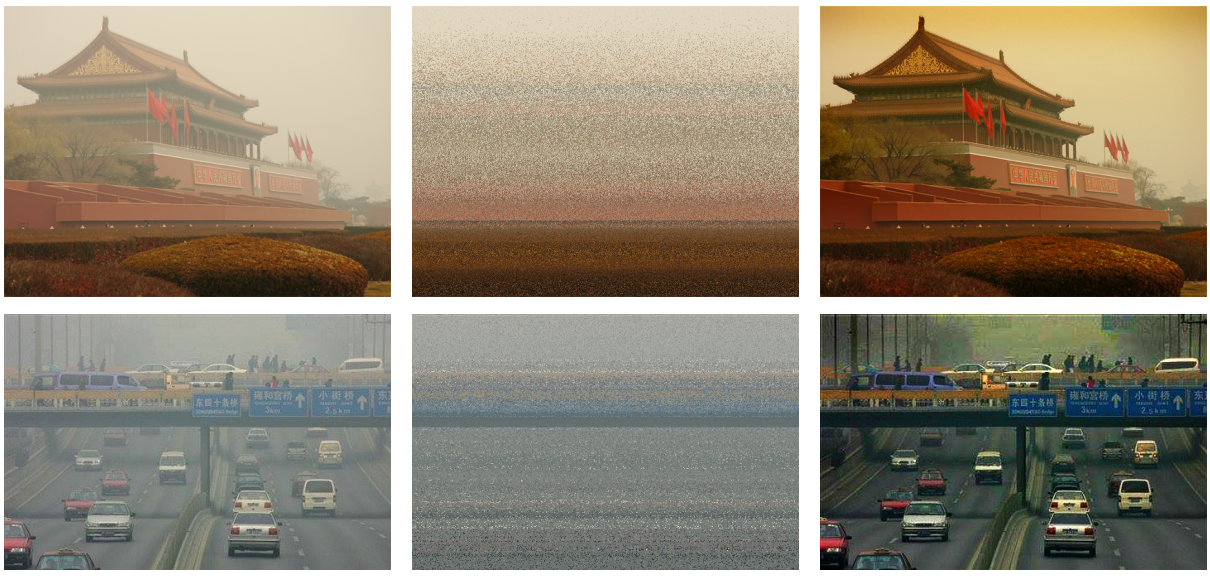
To illustrate how our method work we have used two images (1) chinese.png, a 600 x 450 image and (2) cars.jpg, a 468 x 309 image. These images took 2-3 second to process on an 5th gen i7 processor, run on an OS X, having 16 GB RAM.

3.2 Chaotic Maps

The value of $x(0)$ for the chaotic maps used is a randomly generated floating number between 0 and 1.

3.2.1 Row Interchange

Figure (3) is used to show the results of using row chaotic maps. In Figure 3(b), it can be seen the encrypted image gives away details of the original images. Even though the level of security is less, Figure 3(c), clearly shows that the quality haze removal is excellent.

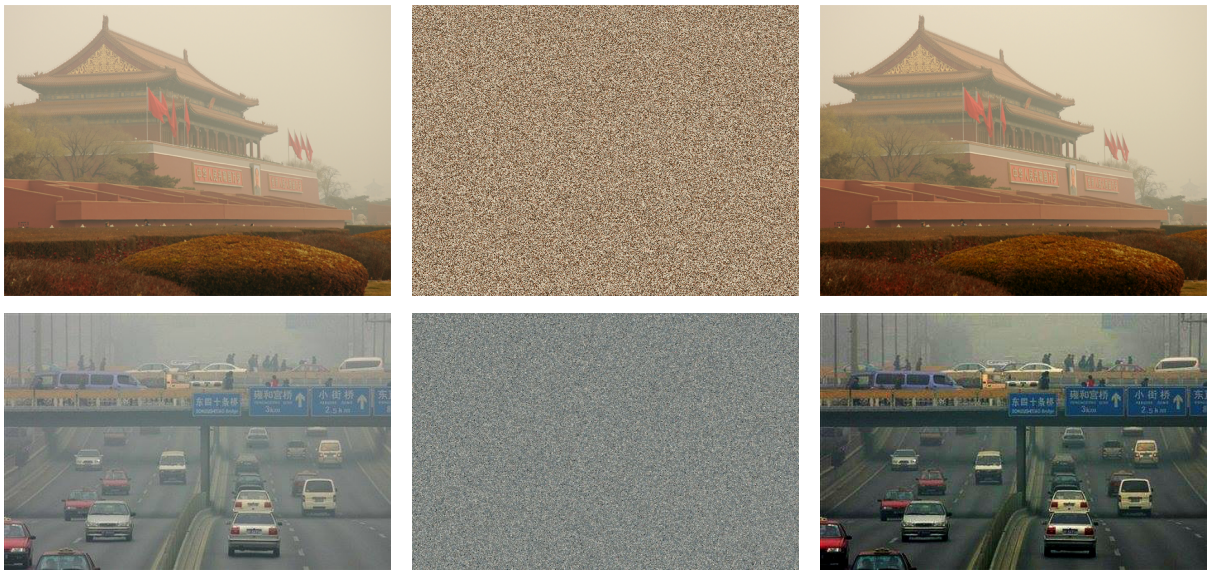


(a) (b) (c)

Figure 3. (a) Original Image. (b) Encrypted Image (c) Image formed after haze removal by our approach.

3.2.2 Row and Column Interchange

Figure (4) shows our results when the chaotic map is applied to both rows and columns. It can be observed from the encrypted image, Figure 4(b) that the level has risen than that in the case of only rows. Although the amount of haze removed gets reduced and the output images obtained are not as good as before.



(a) (b) (c)

Figure 4. (a) Original Image. (b) Encrypted Image (c) Image formed after haze removal by our approach.

3.2.3 Box

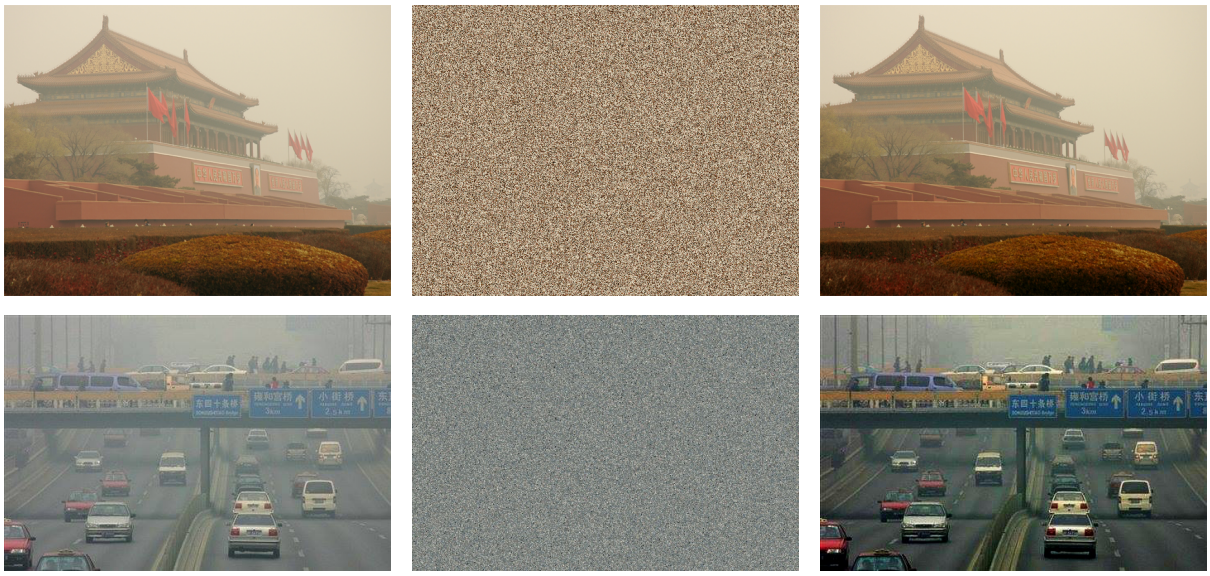
The results of box chaotic have been highlighted in Figure (5). After trying various box sizes we found out the box size of 25 to be able provide a balance between the quality of encryption and haze removed. In this case the encrypted image is still not of good quality as boxes can easily be distinguished. Also in the processed image box patterns can be observed. These may be removed by going in the Fourier domain and applying the notch filter, but as each image has a distinct Fourier Spectrum, it proves to be a computational challenge that we were unable to implement as of now.

(a) (b) (c)

Figure 5. (a) Original Image. (b) Encrypted Image (c) Image formed after haze removal by our approach.

3.2.4 Zig Zag Diffusion

The results of Zig Zag Diffusion [8] have been highlighted in Figure (6). In this approach we applied the chaotic map on the image in the zig-zag pattern. The level of encryption and haze removed was similar to that in the case of rows and columns. On further applying diffusion on the pixels in the encrypted domain increase the security values but only by a small amount.



(a) (b) (c)

Figure 6. (a) Original Image. (b) Encrypted Image (c) Image formed after haze removal by our approach.

3.2 Security Analysis

Table I records the observations of the encryption values for the image "*chinese.png"* and Table 2 shows the encryption values for *"cars.jpg"*. The NPCR(Number of pixels changing rate), Correlation of adjacent (horizontal, vertical and diagonal) pixels, Entropy values and the UACI(Unified average changing intensity) values.

Table 1 (chinese.png)

	Rows Only	Row + Column	Box	Zig-Zag
Correlation - Horizontal	0.848	0.010	0.944	0.094
Correlation - Vertical	0.838	0.090	0.941	0.101
Correlation - Diagonal	0.842	0.084	0.945	0.093
NPCR	95.76	99.12	92.14	99.12
UACI	9.23	25.68	5.02	25.70
Entropy	7.638	7.638	7.638	7.638

Table 2 (cars.jpg)

	Rows Only	Row + Column	Box	Zig-Zag
Correlation - Horizontal	0.575	-0.028	0.814	0.0073
Correlation - Vertical	0.584	-0.00045	0.828	0.015
Correlation - Diagonal	0.573	-0.00079	0.806	0.0027
NPCR	96.54	98.69	96.79	98.68
UACI	5.68	10.45	8.81	10.45
Entropy	6.531	6.532	6.516	6.532

4. CONCLUSION

Shamir Secret Sharing Technique fails to prove to be a good method as it gives an obfuscated output image even though it provides high security values. While applying chaotic maps any attempt to increase the security of the encrypted image resulted in the reduction of the quality of haze removal and vice versa.

5. REFERENCES

[1] KAUR, Er.Sukhdeep; KAUR, Er.Navleen. REVIEW ON VARIOUS HAZE REMOVAL TECHNIQUES. International Journal of Advanced Research in Computer Science, [S.l.], v. 8, n. 5, p. 2683-2687, june 2017

[2] K. He, J. Sun and X. Tang, "Single Image Haze Removal Using Dark Channel Prior," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 12, pp. 2341-2353, Dec. 2011.

[3] S. Pei and T. Lee, "Effective image haze removal using dark channel prior and post-processing," *2012 IEEE International Symposium on Circuits and Systems*, Seoul, 2012, pp. 2777-2780.

[4] *Shari Thomas,* Haze Video Recovery using Guided Filtering

[5] Schettini, R., Gasparini, F., Corchs, S., Marini, F., Capra, A. and Castorina, A., 2010. Contrast image correction method. *Journal of Electronic Imaging*, *19*(2), p.023005.

[6] https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

[7] Singh, Priyanka, Balasubramanian Raman, and Manoj Misra. "Just process me, without knowing me: a secure encrypted domain processing based on Shamir secret sharing and POB number system." *Multimedia Tools and Applications* (2017): 1-25.

[8] Sathishkumar, G.A. and Sriraam, D.N., 2011. Image encryption based on diffusion and multiple chaotic maps. *arXiv preprint arXiv:1103.3792*.