

## **Novel Approach to Image Steganalysis (A Step against Cyber Terrorism)**

**Kaustubh Choudhary**

*Scientist, Defence Research and Development Organisation (DRDO), Naval College of Engineering, Indian Naval Ship Shivaji, Lonavla, Maharashtra, India*

**Abstract:** *Steganography is a technique of hiding secret messages in the image in such a way that no one apart from the sender and intended recipient suspects the existence of the message. Image Steganography is frequently used by Terrorist Networks for securely broadcasting, dead-dropping and communicating the secret information over the internet by hiding the secret information in the Images. As a result it becomes the most preferred tool to be used by Terrorists and criminal organizations for achieving secure CIA (Confidentiality, Integrity and Availability) compliant communication network capable of penetrating deep inside the civilian population. Steganalysis of Image (Identification of Images containing Hidden Information) is a challenging task due to lack of Efficient Algorithms, High rates of False Alarms and above all the High Computation Costs of Analyzing the Images. In this paper a Novel Technique of Image Steganalysis is devised which is not only Fast and Efficient but also Foolproof. The results shown in the paper are obtained using programs written in MATLAB© Image Processing Tool Box.*

**Key Words:** *Bit Plane Slicing, Cyber Crime, Global Terrorism, Image Steganalysis, LSB Insertion, Pixel Aberration, SDT based Image Steganography.*

### **I. Introduction**

Image based steganography is a technique of hiding secret messages in the image in such a way that no one apart from the sender and intended recipient suspects the existence of the message. It is based on invisible communication and this technique strives to hide the very presence of the message itself from the observer. As a result it has been used more frequently by various criminal and terrorist organizations than anybody else. [1][2][3]. Various agencies even claim that 9/11 attacks have been masterminded and planned using image based steganography [4]. Image Steganography offers numerous advantages to the terrorists like Anonymity, Electronic Dead Dropping, Secure Broadcasting and above all very high Secrecy and Security.[5] Thus an innocent looking digital image on any Web Portal, Online Auction Site or even a Social Networking Site may be probably hiding a malicious and deadly terrorist plan or any other significant criminal Information. The Steganalysis is the process of identifying such malicious Stego-images (original image which is used for hiding data is called the Cover-Image whereas the image obtained after inserting the Secret Information in it is called Stego Image) from the bulk of innocent images. The next step of steganalysis involves either the extraction of the hidden information or destroying the information by adding visually imperceptible noise in the image or can be even used for embedding counter-information in the Stego-Image. Considering the voluminous bulk of images flowing every day through the Internet and amount of time and Computation Cost required for analyzing the Image the very first step of identifying an innocent looking Image as a Stego Image becomes the most challenging part of any Steganalysis procedure. It is because we do not have any foolproof method for crisply identifying a steganographic signature in the innocent looking stego-image.

In this paper a technique has been devised for identification of any such stego-image if the Data is hidden in it using Spatial Domain Steganography or LSB Insertion technique. But before moving further it becomes quite necessary to explain the Spatial Domain Image Steganography in brief (elaborately explained in section 2 and Section 3 of [5]). A Digital image consists of numerous discrete pixels. Color of any pixel depends upon the RGB Values of the pixel. For example in a 24 bit BMP image RGB values consists of three 8 bits for each R,G and B and thus a pixel is a combination of 256 different shades (ranging from intensity level of 0 to 255) of red, green and blue intensity levels resulting in 256 x 256 x 256 or more than 16 million colors. Thus if the least significant bits in the R, G and B value are changed the pixel will have minimal degradation of 2/256 or 0.78125%. This minor degradation is psycho-visually imperceptible to human eye due to limitations in Human Visual System (HVS). But at the cost of this negligible degradation 3 bits (1 bits each from red, green and blue) are extracted out of every pixel for transmitting our secret information.

The most of the Spatial Domain Image steganographic techniques use LSB Insertion for hiding data in the image. But some Spatial Domain techniques instead of using LSB use around five to seven bits of the pixels and thus make large changes in the RGB Values of the pixel. As a result the entire information gets concentrated in few pixels. Although changes in the pixel are quite large but since pixels are very small in size and also

because very few pixels change so these changes go unnoticed by human eye. Moreover most of these Concentrating Algorithms change the pixels of only the bottom few rows. This is because our human brain concentrates more on the top, center and other important features of the image than on the bottom rows. There are many variants of Spatial Domain Steganography but all of them can be broadly classified into these two types only and is further elaborated in Section 2 of this paper. There are other techniques also for hiding data in the image. For example Transformation Domain Steganography may use Discrete Cosine Transforms or Discrete Wavelet Transform for embedding data and some other steganographic algorithm may use a different color space itself (Example RGB may be converted to YCbCr and then various steganographic techniques can applied). But the scope of this paper is limited to Foolproof Steganalysis of only Spatial Domain Steganography. For Steganalysis of Spatial Domain Stego-images various methods like Brute Force Attacks, Pattern Matching, Statistical Attack (Histogram, Kurtosis), Mathematical Approaches (Stir Mark Attack) and Transform Domain Attacks are available. Most of them are highly unreliable because they either produce frequent false alarms or do not identify the stego-image itself. Whereas other advanced steganalysis techniques based on Stir Mark Attack [6] and Gabor Filtering [7] are very expensive in terms of Computational Power and time. The weaknesses of these steganalysis algorithms are elaborated in Section 5.2.3 of [5]. Thus most spatial domain steganalysis algorithms suffer from one of the two weaknesses. Either they are unreliable and ineffective or else they are computationally very expensive and slow. To overcome these limitations two different approaches to steganalysis have been proposed in this paper. Both these approaches are computationally very fast and complement each other and thus together they form an Efficient, Effective and Reliable technique of Spatial Domain Steganalysis of Images. Both these techniques not just identify the Stego image but also informs the locations of the pixels having information and also provides the information in the binary form.

## II. Steganalysis Technique Proposed

As mentioned in Section 1 most spatial domain image steganographic algorithms can be broadly classified into two types. Either they concentrate the secret information in few pixels or they distribute the information in large number of pixels. Those algorithms which concentrate the information bring large and noticeable changes in very few pixels (sometimes Information appears as grains in the bottom most row of the image) by using around five to seven bits of the pixel. They use bottom most row is due to psycho-visual weaknesses of the human brain and gets explained from Figure 2. Such steganographic algorithms will be here onwards referred as Concentrating Steganographic Algorithms.



Fig 1 Large and Perceptible changes in the pixels (Grains) go unnoticed in the Last Row of the Image

On the other hand those algorithms which distribute the information in large number of pixels make very small and imperceptible changes in the pixels by using either one or two Least Significant bits for storing information in the pixels. Such steganographic algorithms will be here onwards referred as in this paper as Distributing Steganographic Algorithms.

### 2.1 Steganalysis of Concentrating Steganographic Algorithms

In any natural image the pixels do not change abruptly and color of any pixel is dependent on the color of the neighboring pixels thus the pixels are auto-correlated. Thus if any pixel is substantially different from its neighboring pixels then it indicates that the given innocent looking image is a stego-image. But it is equally true that two neighboring pixels are not necessarily same or else the image will not be formed. But two pixels which are neighbors will not be very different also. Moreover the average difference between the concerned pixel and its neighbors will be within the range of difference among the neighbors themselves. The difference between the pixels implies the individual difference of each R, G and B components of the pixels and not the mean of R, G and B because the averaging effect will lead to loss of vital information.

In Figure 2 any arbitrary pixel  $P_{i,k}$  or  $P(i,k)$  (Pixel located at  $i^{\text{th}}$  row and  $j^{\text{th}}$  column of the image) is shown along with its 8 neighbors.

The differences among the Adjacent Neighbors of the pixel  $P_{i,k}$  or  $P(i,k)$  is given as  $P(i-1,k-1) - P(i-1,k) = A_1$ ,  $P(i-1,k) - P(i-1,k+1) = A_2$ ,  $P(i-1,k+1) - P(i,k+1) = A_3$ ,  $P(i,k+1) - P(i+1,k+1) = A_4$ ,  $P(i+1,k+1) - P(i+1,k) = A_5$ ,  $P(i+1,k) - P(i+1,k-1) = A_6$ ,  $P(i+1,k-1) - P(i,k-1) = A_7$  and  $P(i,k-1) - P(i-1,k-1) = A_8$ .

The difference of the pixel  $P(i,k)$  with its neighbors is given as  $P(i-1,k-1) - P(i,k) = D_1$ ,  $P(i-1,k) - P(i,k) = D_2$ ,  $P(i-1,k+1) - P(i,k) = D_3$ ,  $P(i,k+1) - P(i,k) = D_4$ ,  $P(i+1,k+1) - P(i,k) = D_5$ ,  $P(i+1,k) - P(i,k) = D_6$ ,  $P(i+1,k-1) - P(i,k) = D_7$  and  $P(i,k-1) - P(i,k) = D_8$ .

Since the adjacent neighbors are not necessarily same so  $A_1 = A_2 = A_3 = \dots = A_8$  is not necessary. But in any natural image the average of the difference between the Pixel concerned ie  $P(i,k)$  from its neighbors given by mean of  $D_1, D_2, D_3, \dots, D_8$  and represented as  $\bar{D}$  should lie well within the range of differences among its neighbors themselves ie  $A_1, A_2, A_3, \dots, A_8$ . Thus any pixel is as much different from its neighbors as the neighbors themselves are.

$P_{i-1,k-1}$	$P_{i-1,k}$	$P_{i-1,k+1}$
$P_{i,k-1}$	$P_{i,k}$	$P_{i,k+1}$
$P_{i+1,k-1}$	$P_{i+1,k}$	$P_{i+1,k+1}$

Fig 2 Pixel  $P_{i,k}$  and its neighbors

The degree of difference of the pixel  $P(i,k)$  from its neighborhood is represented by  $\delta(P(i,k))$  and is called Pixel Aberration of  $P(i,k)$ . This Pixel Aberration is measured in terms of standard deviation of the difference among the Adjacent Neighbors of  $P(i,k)$  (adjacent neighbors of  $P(i,k)$  are the pairs  $\{P(i-1,k-1), P(i-1,k)\}$ ,  $\{P(i-1,k), P(i-1,k+1)\}$ ,  $\{P(i-1,k+1), P(i,k+1)\}$ ,  $\{P(i,k+1), P(i+1,k+1)\}$ ,  $\{P(i+1,k+1), P(i+1,k)\}$ ,  $\{P(i+1,k), P(i+1,k-1)\}$ ,  $\{P(i+1,k-1), P(i,k-1)\}$  and  $\{P(i,k-1), P(i-1,k-1)\}$ ) and is represented as  $\sigma(A)$  and the average difference of  $P(i,k)$  from its neighbors represented as  $\bar{D}$ . In other words the concerned pixel  $P(i,k)$  has to be within the limits of the differences among its neighbors. So  $\delta(P(i,k))$  is the degree of difference of  $P(i,k)$  on an average from its neighbors represented. Thus

$$\bar{D} = \frac{1}{8} \sum_{u=1}^8 D_u$$

$$\bar{A} = \frac{1}{8} \sum_{u=1}^8 A_u \quad \text{and} \quad \sigma(A) = \sqrt{\frac{1}{8} \sum_{u=1}^8 (A_u - \bar{A})^2}$$

$$\delta(P(i,k)) = \frac{\bar{D} - \bar{A}}{\sigma(A)} \tag{1}$$

The value of  $\delta(P(i,k))$  for every pixel in the image should be within the tolerable limits. Thus if the values of  $\delta(P(i,k))$  is plotted for every pixel in the image then the graph should not have sudden high values in a truly innocent image. The plot of  $\delta(P(i,k))$  for every pixel in the image is called Pixel Aberration Plot of the Image. Also the range of  $\delta(P(i,k))$  i.e. the difference of the maximum  $\delta(P(i,k))$  to minimum  $\delta(P(i,k))$  in the image must be low for an innocent image. The more elaborate, mathematical and detailed explanation of the concept of  $\delta(P(i,k))$  is given in Definition 8 to Definition 10 in Section 2.2 and Requirement 3 and Requirement 4 in Section 2.3.1 of [8].

## 2.2 Steganalysis of Distributing Steganographic Algorithms

The distributing steganographic algorithms spread the secret information in large number of pixels. They do so by embedding the information in one or two least significant bit of each pixel. As a result the Information gets broken in to large number of sub-informations and gets stored in the least significant bit of large number of pixels. Thus for all distributing type of steganographic algorithms it can be conclusively said that information resides in at least the least significant bit of the pixels of the stego image (Information may also be present in the second LSB of the pixels too). Thus bit plane slicing of the suspicious image will highlight the presence of any information in the LSB plane of the image. The concept of Bit Plane Slicing is explained in brief in the next section.

### 2.2.1 Bit Plane Slicing

Since we know that every image is made up of pixels and the pixel information (Red, Green and Blue intensity levels) of every pixel is stored in fixed sized memory space corresponding to each pixel. The size of memory and the way the pixel information is stored depends upon the format of the image. For example in a 24 bit BMP image each pixel is stored as three 8 bits corresponding to the intensity levels of the three primary colors i.e. RGB values while other formats may use a entirely different model for storing the pixel information but all of them store the pixel information in the memory corresponding to each pixel. So for the sake of simplicity a 24 bit BMP Image is assumed for explaining Bit Plane Slicing.

Each pixel of a 24 bit BMP Image is stored in the three 8 bits corresponding to three colors. In other words pixel information consists of 8 bit RGB values corresponding to each and every pixel. So the entire image can be thought to be consisting of eight different images or planes corresponding to 8 different bit positions in the RGB value. Thus these 8 different bit-planes highlight the contribution of each of the eight different bit position of the RGB Value to the total image. In other words the entire image is sliced in to 8 images-planes corresponding to each bit of the RGB value and this process is called as Bit Plane Slicing. The bit plane image corresponding to the plane of the most significant bit (MSB) has the maximum contribution to the total image and forms the majority of the visually significant image data and therefore almost represents the total image. The bit-plane images corresponding to other lower bit positions contribute only the subtle details of the image. Whereas the bit-plane image corresponding to the LSB of the RGB value has the minimum contribution of only 1 out of total of 255 Intensity level to the total image. Thus LSB plane of the Image appears black (some variation in black shade can be seen if the image is highly enlarged) due to negligible contribution (of only 1 out of 255 intensity levels) to the total image and is insignificant from the image processing point of view. But in LSB based Image Steganography the secret information is hidden only in the LSB of the RGB Values. Thus the LSB Plane of the image also contains the secret information hidden in the image.

### 2.2.2 LSB Plane has Information

Since the LSB of the RGB values of the image hides the secret information so the pixels forming the LSB Plane of the Image either represent the hidden information or the LSB Component of the total Image. In other words the image corresponding to the contribution of the LSB to the stego-image also contains the secret information. But the intensity levels for any of the R, G or B value of any image in LSB plane is at max 1 which is negligibly small when compared with total of 255 intensity levels. As a result the image in its LSB Plane appears black. So although the LSB Plane of the Stego-Image has maximum concentration of secret information but due to its dark black color we are unable to see the information in the image. As a remedy if the contrast of the LSB Plane of the image can be increased, then we can easily see the information stored in the image. A technique used here is that if any of the R, G or B value of the LSB Plane of the image is 1 then it is replaced by the intensity level of 255 whereas the intensity level of 0 is left unchanged. So the new image obtained has R, G or B value of every pixel as either 255 (if the corresponding true LSB value was 1) or else it remains 0. Therefore the modified LSB Plane of the image will appear multicolored and each pixel of this image will have one of the seven possible colors ranging from three primary colors (Red, Green and Blue), four other colors obtained by their combination i.e. Yellow (R+G), Magenta (R+B) and Cyan (B+G), White (R+G+B) and Black indicating absence of any of the three primary color components. In Figure 3 all these 6 colors (Excluding Black) are shown as a combination of 3 primary colors and also a section of Multicolored LSB Plane of some Image is shown. It can be clearly seen that any pixel of the Multi-Colored LSB plane has only one of those six colors or else it is black in color. Hence hereafter in this

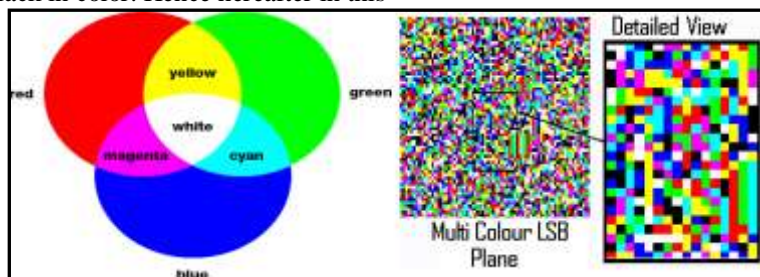


Fig 3 Three Primary Colors and Their Combinations and Multicolored LSB Plane of some Image

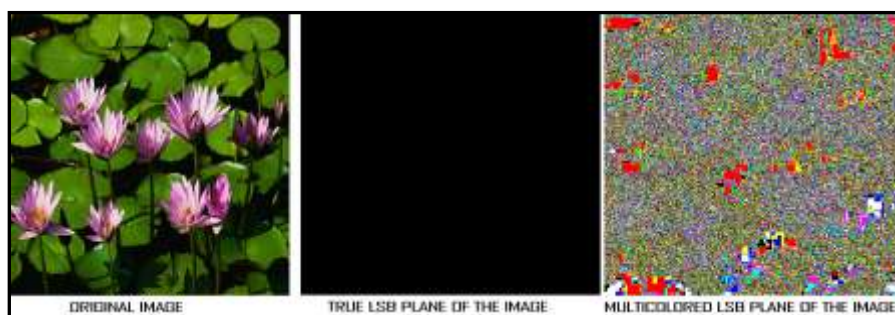


Fig 4 Original Image and Corresponding True LSB and Multicolored LSB Plane (width reduced by 60%)

paper this modified LSB Plane of the image will be referred as Multicolored LSB Plane of the Image. Due to the presence of 7 colors corresponding to each of the LSB value of the image the presence of information in the LSB of the Image can be easily traced even by the visual clues only. In Figure 4 the LSB Plane and Multicolored LSB Plane is show for the same Image.



### III. Results

Three different steganographic algorithms are used for inserting data in the Image. One of them is a Concentrating Algorithm while other two are Distributing Algorithms and referred in the paper as Distributing Algorithm 1 (uses last 2 LSBs of the pixels for inserting data) and Distributing Algorithm 2 (uses only the LSB for inserting data in the pixel).

#### 3.1 Pixel Aberration Analysis:

Two different cover images are used for determination of the results. One of them is smooth i.e. has less overall pixel aberration while other is unsmooth and has high overall pixel aberration. The results of Pixel Aberration Analysis are shown (Figure 5 and Figure 6) as the Pixel Aberration plot for the Cover Image and three associated Stego-Image generated by all the three steganographic algorithms. The Figure 5 uses Smooth image as the Cover Image and Figure 6 uses Unsmooth image as the Cover Image. From Figure 5 and Figure 6 it is clearly evident that Pixel Aberration Analysis conclusively identifies the abnormalities produced by Concentrating Steganographic Algorithms and hence confirms presence of data in all type of Stego-Images obtained by Concentrating type of

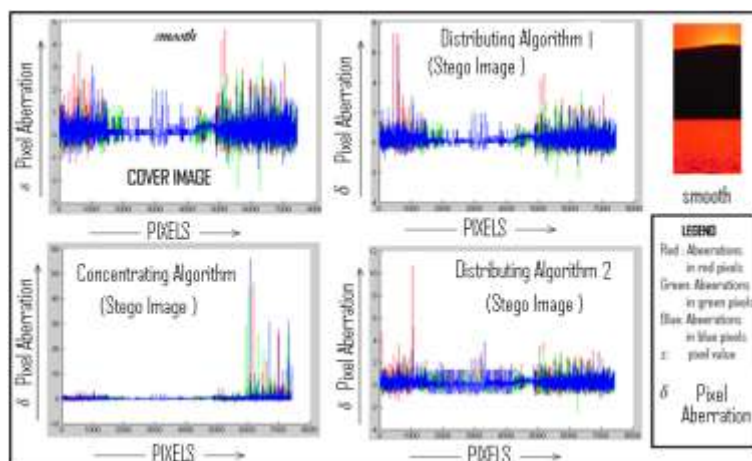


Fig 5 Pixel Aberration Plot of Smooth Cover Image and Associated Stego Images Generated by 3 Algorithms

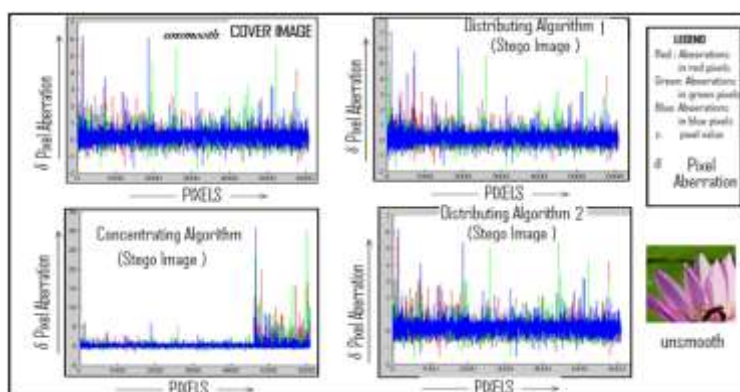


Fig 6 Pixel Aberration Plot of Unsmooth Cover-Image and Associated Stego-Images Generated by 3 Algorithms

Steganographic Algorithm. From Figure 5 we can also conclude that the use of Pixel Aberration analysis, on some occasions can be helpful in steganalysing even distributing type of algorithms (Distributing Algorithm 2) in case of smooth cover images and is proved by sudden high value of pixel aberration at 1000<sup>th</sup> pixel in the stego-image obtained by Distributing Algorithm 2 and is shown in Figure 5. The range of Pixel Aberration in Concentrating Algorithm is much higher than the Distributing Algorithms and thus Pixel Aberration Analysis clearly steganalyses the stego images generated by Concentrating Algorithms and is proved by the Pixel Aberration Plots of the stego-image obtained by Concentrating Algorithm in both Figure 5 and Figure 6. Pixel Aberration Analysis is given in much more detail in [8] i.e. in Definition 7 to Definition 10 of Section 2.2, Requirement 3 and Requirement 4 of Section 2.3.1 and Section 3.1 of [8].

#### 3.2 Analysis based on Multicolored LSB Plane Imaging

Although Pixel Aberration Analysis is a foolproof method of steganalysis the stego images generated by Concentrating Steganographic Algorithms but it may fail in case of Distributing type of Steganographic Algorithms. As a remedy the Multicolored LSB Plane Analysis of the stegoimage comes handy in Steganalysis

of the Distributing type of Steganographic Algorithms. In Figure 7 the Multicolored LSB Planes of stego images obtained by the distributing steganographic algorithm using four different cover images are shown. The secret information is inserted in three different ways in all the four Cover Images. In first case a string with single character 'a' of length 600 is inserted, that is aaaaaa.....aaa (600 times), in second case a repeating string of total length 600 is inserted i.e. abcdefgh...xyz1234..... abcdefgh...xyz1234 (20 times) where as in the third case a true information is embedded i.e. the first paragraph of section 1 of this paper consisting of 863 characters (including spaces). From the distortions in the Multicolored LSB Planes of the three Stego Images corresponding to every Cover Image in Figure 7 it can be conclusively said that these Stego-Images contain information.

Every character in the information is encoded by a unique binary code and every unique binary code corresponds to a unique (in color) set of pixels in the LSB Plane of the stego image. The pixels corresponding to the binary code of information are called Information Pixels and all other pixels in the Multicolored LSB Plane are the LSB Components of the image and hence are Image Pixels. Thus we can say that Multicolored LSB Plane of the Stego-Image consists of two different types of pixels. One category of pixels corresponds to Secret Information only while the other category of pixels in the Multicolored LSB Plane of the Stego-Image corresponds to the LSB of the cover image only and therefore both the categories of the pixels (Information and Image) are clearly very different. In other words the entire hidden information in the stego-image gets represented as a distinct category of Pixels in the Multicolored LSB Plane of the Image. Thus the Multicolored LSB Plane of the Stego Image consists of pixels corresponding to the Cover Image and also the Pixels corresponding to the Information. For conclusively distinguishing the Information pixel from the pixel corresponding to LSB of the Image in the Multicolored LSB Plane of the Stego Image, the pixel properties of Information as well as the LSB of the image must be determined.

After studying the multicolored LSB Planes of more than 200 test images it was concluded that multicolor LSB Plane of any image (even stego image) consists of combination of four main types of pixels clusters. The majority of the pixels (approximately 70 to 100% of the complete image) of the Multicolored LSB Plane consists of numerous co-located multicolored pixels (i.e. pixels of different colors are located as immediate neighbors) and thus appears Fine Grained and hence are called Fine Grained Pixel Clusters in this paper. Other pixels clusters are also classified on the basis of degree of neighboring of differently colored pixels and thus belong to Coarse Grained Pixel Clusters (pixels of same color occurring as immediate neighbors but at larger distances have different pixel colors), Boulder Grained Pixel Clusters (pixels of same color appearing continuously in linear or circular or any other pattern interspersed with pixels of other colors) and Continuous Pixel Clusters (the entire plane consists of pixels of same color). These pixel clusters may have some background color also. In Fig 8 the four different pixel clusters are shown along with a Multicolored LSB Plane of some Image (of a Person's Face).

The pixels corresponding to the Information in the Multicolored LSB Plane of the Stego-Image are clustered generally as Fine Grained and very occasionally may congregate as Coarse Grained. Considering the fact that information consists of many different characters and each character is represented by a unique set of pixels so information pixels never get clustered as Boulder Grains or Continuous Grains. In other words Boulder Grained or Continuous Grained clustering of pixels will happen only when the same type (color) of pixels aggregate at one particular location which cannot happen for Information Pixels. So in the Multicolored LSB plane of the Stego Image the presence of Information in the Continuous Grained and Boulder Grained Pixels is immediately ruled out. Thus only group of pixels which still remain suspicious are mainly the Fine Grained and to some extent the Coarse Grained Pixels.

It was observed that in most of the innocent images (190 out of 200 test images) the Fine Grained and Coarse Grained Pixels (sampled as square or rectangle) in the Multicolored LSB Plane of the Innocent Image have equal

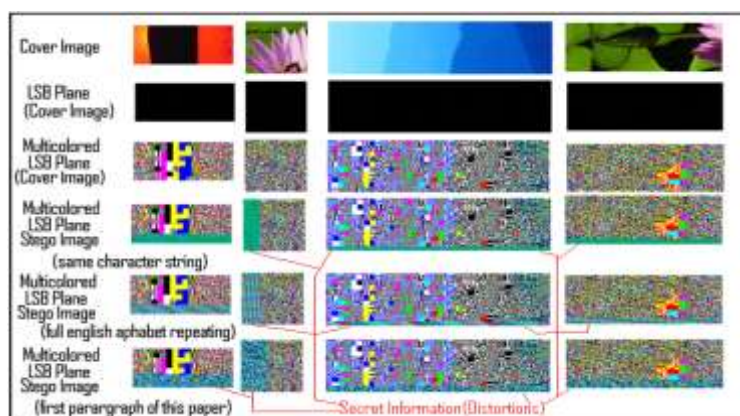


Fig 7 Multicolored LSB Planes of four different Cover Images and three associated stego images

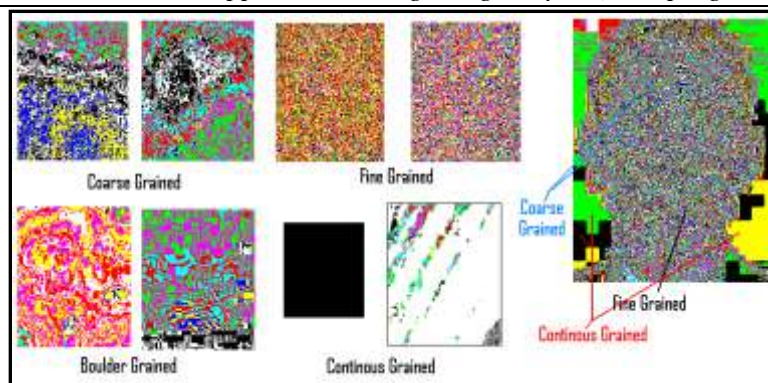


Fig 8 Types of Pixel Clusters in the Multicolored LSB Plane of any Image

distribution of Red, Green and Blue components. This was found to be true even for those fine grained and coarse grained pixel clusters which had some prior background color too. Thus the number of pixels with Red Intensity as 255 was found to be almost equal to the number of pixels with Green Intensity as 255, which in turn was almost equal to the number of pixels with Blue Intensity as 255 (generally around 50% of the total number of pixels but not always). This condition applied even on the LSB components or Image pixels of the Multicolored LSB Plane of the Stego-Image too.

On the other hand the Information pixels in the Multicolored LSB Plane of the Stego-Image were not seen to obey the previously mentioned criteria of equal distribution of Red, Green and Blue components. Thus the Red, Green and Blue Components of the Information Pixels in the Multicolored LSB Plane of the Stego-Image were found to be unequally distributed. The reason for this is that in any genuine information (assuming English language) certain characters like blank spaces, all vowels (as per order of occurrence e, a, o, i, and u) and some consonants t, n, s, h, r, d, c (as per order of occurrence) occur more frequently than other characters. Since each character corresponds to a unique (in terms of color) set of pixels and as the distribution of characters is not uniform in the Information so Information Pixels do not have equally distributed Red, Green and Blue components in the Pixels.

These properties of Information Pixel and Image Pixels were concluded by experimenting on 200 images but due to space constraints the results of the experiments on few selected images are summarized in four Tables i.e. Table 1, Table 2, Table 3 and Table 4. All the four tables contain the Multicolored LSB Plane of the Image, the values of R, G and B components in the Multicolored LSB Plane, The ratio R:G:B and the Bias (i.e the degree of deviation R:G:B from ideal distribution of R:G:B = 1:1:1). The Bias is 0 if R:G:B = 1:1:1 and is calculated by subtracting the sum of the ratios of R:G:B from 3 i.e. if the ratio of the three primary colors in the Multicolored LSB Plane is R:G:B, then error is  $3 - (R+G+B)$ .

The Table 1 contains only those sections of the Multicolored LSB Plane of the image which follow approximately 1:1:1 distribution of Red, Green and Blue components in the Multicolored Plane of the Image. The majority of the pixels in the everyday image are composed of Least Significant Bits corresponding to the Multicolored LSB sections given in Table 1. While in Table 2 those sections of the Multicolored LSB Plane of the image are given which are quite different from 1:1:1 distribution of the Red, Green and Blue components and such sections are rarely seen in few images and occurs primarily due to any bias in the complete image which can be easily understood by analyzing the complete image. In this paper such Images will be referred as Rare Occurring Biased Images. In Table 3 and Table 4 the sections corresponding to the Information Pixels obtain by Algorithm 1 (2 bit LSB Insertion) and Algorithm 2 (1 bit LSB Insertion) respectively in the Multicolored LSB Plane of the Image is given and they have Red, Green and Blue Components significantly different from 1:1:1 distribution.

The majority of pixels in any image are composed of sections corresponding to Table 1 and the average Bias (deviation from R: G: B = 1:1:1) in Table 1 is 0.035067. The average Bias in table 2 (which corresponds to the pixel clusters corresponding to Rare Occurring Biased Images which do not obey R: G: B = 1:1:1) is 0.3438. As expected the average deviation from R:G:B = 1:1:1 in the Information Pixels was considerably high and is proved by the high values of average deviation in Table 3 and Table 4. The average Bias in Table 3 is 0.670829 where as average Bias in Table 4 is 0.830675. The average Bias in Table 3 is lower than Table 4 because Table 3 corresponds to the Information pixels obtained by Distributing Algorithm 1 which performs 2 bit LSB Insertion where as the Table 4 corresponds to Information pixel obtained by Distributing Algorithm 2 which performs 1 bit LSB Insertion. As a result the concentration of Information in the LSB (Multicolored LSB Plane of the Stego Image) is more in Distributing Algorithm 2 than Distributing Algorithm 1. Therefore the average Bias (deviation from R:G:B = 1:1:1) is higher in Table 4 (Distributing Algorithm 2) than Table 3 (Distributing Algorithm 1).

It is worth mentioning that although there are certain rare fine grained pixel clusters (seen in Rare Occurring Biased Images) which do not obey R:G:B = 1:1:1 property but even then the degree of deviation from



R:G:B = 1:1:1 in Information Pixels is far higher than the degree of deviation from R:G:B =1:1:1 in fine grained pixel clusters corresponding to Rare Occurring Biased Images. This can be understood from Figure 9 which is the graph corresponding to the degree of deviation from R:G:B = 1:1:1 (obtained by sampling 100 x 100 pixel clusters) in Biased Cover Image and Biased Stego Image. The Rare Occurring Biased image used in Figure 9 is one such image which had highest degree of Bias (0.3099) among all 200 test image samples and the properties of certain section (9200 Pixel Section) of this image is shown in the first row of the Table 2. The mean weighted deviation in the biased cover image was just 0.3099 where as the mean weighted deviation in biased stego image was 0.6846. The same can be concluded from the graphs in Figure 9.

In Figure 10 the Multicolored LSB Planes of different Stego Images obtained by Algorithm 1 and Algorithm 2 are given and Information can be clearly seen in all the Stego Images.

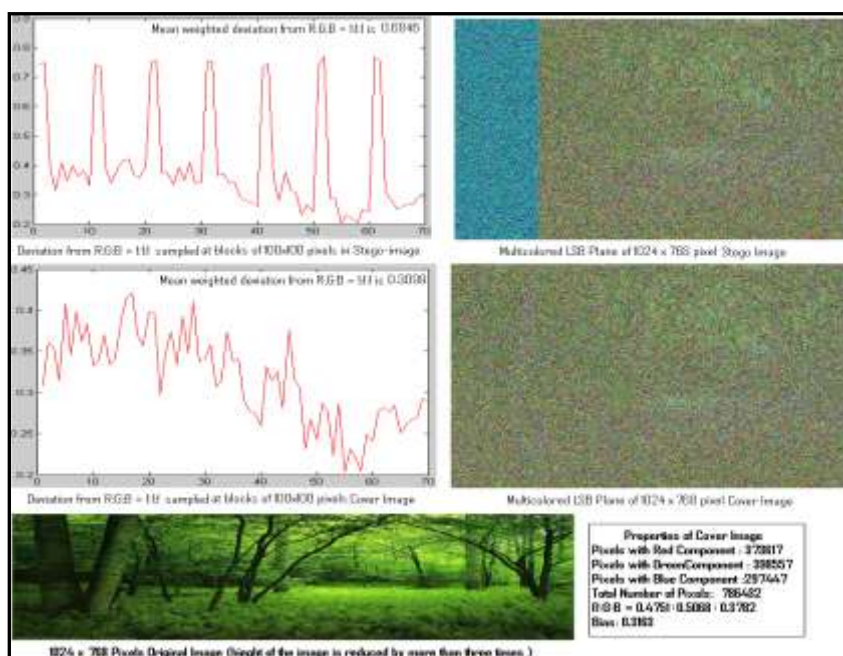





Fig 9 Deviation from R:G:B = 1:1:1 is much higher even in the Biased Stego Image than the Biased Cover Image

Multicolor LSB Plane	RGB Components	Ratio	Bias
	R Count: 12234 G Count: 11956 B Count: 12167 Total Pixels: 24616 R Percentage: 49.6994 G Percentage: 48.5700 B Percentage: 49.4272	R : G : B = 1: 0.9773 : 0.9945	0.0282
	R Count: 59459 G Count: 64921 B Count: 63362 Total Pixels: 114597 R Percentage: 51.8853 G Percentage: 56.6516 B Percentage: 55.2912	R : G : B = 0.9159 : 1 : 0.9760	0.1081
	R Count: 15272 G Count: 15363 B Count: 15239 Total Pixels: 30504 R Percentage: 50.0656 G Percentage: 50.3639 B Percentage: 49.9574	R : G : B = 0.9941 : 1 : 0.9919	0.0140





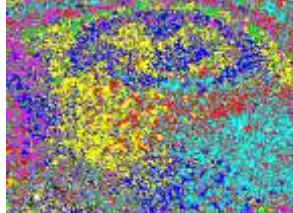
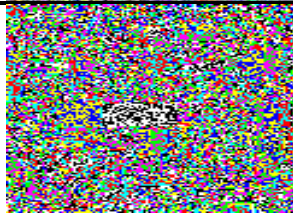

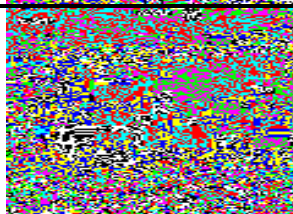

	R Count: 102903 G Count: 106345 B Count: 105183 Total Pixels: 210535 R Percentage: 48.8769 G Percentage: 50.5118 B Percentage: 49.9599	R : G : B = 0.9676 : 1 : 0.9891	0.0433
	R Count: 13087 G Count: 13166 B Count: 13136 Total Pixels: 26364 R Percentage: 49.6397 G Percentage: 49.9393 B Percentage: 49.8255	R : G : B = 0.9940 : 1 : 0.9977	0.0083
	R Count: 69101 G Count: 71629 B Count: 70830 Total Pixels: 137808 R Percentage: 50.1430 G Percentage: 51.9774 B Percentage: 51.3976	R : G : B = 0.9647 : 1 : 0.9888	0.0464
	R Count: 8236 G Count: 8320 B Count: 8268 Total Pixels: 16510 R Percentage: 49.8849 G Percentage: 50.3937 B Percentage: 50.0787	R : G : B = 0.9899 : 1 : 0.9938	0.0163
	R Count: 9788 G Count: 9812 B Count: 9672 Total Pixels: 19404 R Percentage: 50.4432 G Percentage: 50.5669 B Percentage: 49.8454	R : G : B = 0.9976 : 1 : 0.9857	0.0167
	R Count: 9370 G Count: 9173 B Count: 9189 Total Pixels: 18450 R Percentage: 50.7859 G Percentage: 49.7182 B Percentage: 49.8049	R : G : B = 1 : 0.9790 : 0.9807	0.0403
	R Count: 11574 G Count: 11635 B Count: 11651 Total Pixels: 23184 R Percentage: 49.9224 G Percentage: 50.1855 B Percentage: 50.2545	R : G : B = 0.9934 : 0.9986 : 1	0.0080

Table 1 Sections from Multicolor LSB Planes of Images obeying 1:1:1 Rule (majority of Pixels obey this rule)



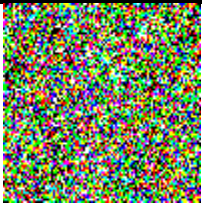
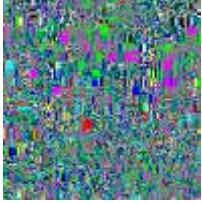

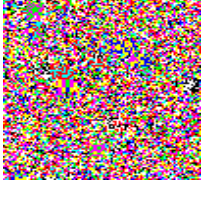
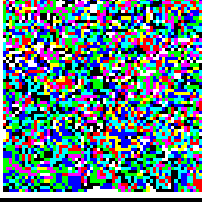
Multicolor Plane	LSB	RGB Components	Ratio	Bias
		R Count: 4266 G Count: 4594 B Count: 3316 Total Pixels: 9200 R Percentage: 46.3696 G Percentage: 49.9348 B Percentage: 36.0435	R : G : B = 0.9286 : 1 : 0.7218	0.3496
		R Count: 8071 G Count: 11027 B Count: 10987 Total Pixels: 21976 R Percentage: 36.7264 G Percentage: 50.1775 B Percentage: 49.9954	R : G : B = 0.7319 : 1 : 0.9964	0.2717
		R Count: 4162 G Count: 4571 B Count: 3328 Total Pixels: 8811 R Percentage: 47.2364 G Percentage: 51.8783 B Percentage: 37.7710	R : G : B = 0.9105 : 1 : 0.7281	0.3614
		R Count: 13443 G Count: 18515 B Count: 19188 Total Pixels: 37600 R Percentage: 35.7527 G Percentage: 49.2420 B Percentage: 51.0319	R : G : B = 0.7006 : 0.9649 : 1	0.3345
		R Count: 11006 G Count: 11339 B Count: 8759 Total Pixels: 22576 R Percentage: 48.7509 G Percentage: 50.2259 B Percentage: 38.7978	R : G : B = 0.9706 : 1 : 0.7725	0.2569
		R Count: 8173 G Count: 6239 B Count: 6159 Total Pixels: 12322 R Percentage: 66.3285 G Percentage: 50.6330 B Percentage: 49.9838	R : G : B = 1 : 0.7634 : 0.7536	0.4831
		R Count: 1585 G Count: 2213 B Count: 2301 Total Pixels: 4556 R Percentage: 34.7893 G Percentage: 48.5733 B Percentage: 50.5048	R : G : B = 0.6888 : 0.9618 : 1	0.3494

Table 2 Sections from Multicolor LSB Planes of Images which do not obey 1:1:1 Rule (rarely seen in some images)

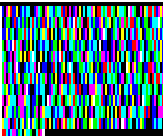
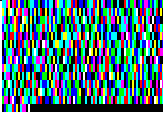
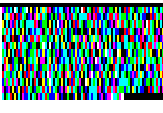
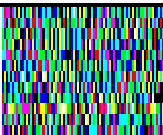
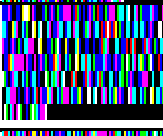


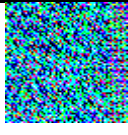
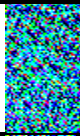
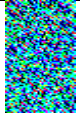
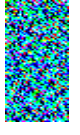
Multicolor Plane	LSB	RGB Components	Ratio	Bias	Information hidden in the Image
		R Percentage: 24.7917 G Percentage: 42.5000 B Percentage: 48.6458 Total Pixels: 960	R : G : B = 0.5096 : 0.8737 : 1	0.6167	Paragraphs from section 1
		R Percentage: 25.3571 G Percentage: 42.5000 B Percentage: 45.5357 Total Pixels: 1120	R : G : B = 0.5569 : 0.9333 : 1	0.5098	Paragraphs from section 2.1
		R Percentage: 25.5769 G Percentage: 45.3846 B Percentage: 45.4808 Total Pixels: 1040	R : G : B = 0.5624 : 0.9979 : 1	0.4397	Paragraphs from section 2.2
		R Percentage: 26.8269 G Percentage: 45.8654 B Percentage: 45.8654 Total Pixels: 1040	R : G : B = 0.5849 : 1 : 1	0.4151	Paragraphs from section 3.2
		R Percentage: 22.1429 G Percentage: 28.2143 B Percentage: 49.6429 Total Pixels: 560	R : G : B = 0.4460 : 0.5683 : 1	0.9856	Message in Hindi
		R Percentage: 26.9643 G Percentage: 33.2143 B Percentage: 53.0357 Total Pixels: 560	R : G : B = 0.5084 : 0.6263 : 1	0.8653	Message in Tamil
		R Percentage: 30.8333 G Percentage: 31.6667 B Percentage: 55.0000 Total Pixels: 240	R : G : B = 0.5606 : 0.5758 : 1	0.8636	Message in Gujarati

Table 3 Multicolor LSB Planes of Information Pixels obtained by Distributing Algorithm 1 (2 Bit LSB Insertion)

Multicolor Plane	LSB	RGB Components	Ratio	Bias	Information hidden in the Image
		RPercentage: 20.9420 GPercentage: 54.2369 BPercentage: 63.7959 Total Pixels: 4331	R : G : B = 0.3283 : 0.8502 : 1	0.8216	Paragraphs from section 1
		RPercentage: 19.5886 GPercentage: 53.5759 BPercentage: 63.2911 Total Pixels: 3160	R : G : B = 0.3095: 0.8465 : 1	0.8440	Paragraphs from section 2.1
		RPercentage: 20.7500 GPercentage: 55.0000 BPercentage: 63.3214 Total Pixels: 2800	R : G : B = 0.3277: 0.8686 : 1	0.8037	Paragraphs from section 2.2
		RPercentage: 19.9194 GPercentage: 53.9113 BPercentage: 63.2258 Total Pixels: 2480	R : G : B = 0.3151 : 0.8527 : 1	0.8323	Paragraphs from section 3.2



	RPercentage: 19.6318 GPercentage: 53.1486 BPercentage: 59.9008 Total Pixels: 65934	R : G : B = 0.3277: 0.8873 : 1	0.785 0	This Entire Paper is hidden as Information.
	RPercentage: 16.5479 GPercentage: 54.9041 BPercentage: 62.1370 Total Pixels: 1825	R : G : B = 0.2663: 0.8836 : 1	0.850 1	Message in Hindi
	RPercentage: 18.8889 GPercentage: 54.4444 BPercentage: 64.3889 Total Pixels: 1800	R : G : B = 0.2934 : 0.8456 : 1	0.861 1	Message in Tamil
	RPercentage: 19.5618 GPercentage: 52.6343 BPercentage: 62.6500 Total Pixels: 1917	R : G : B = 0.3122 : 0.8401 : 1	0.847 6	Message in Gujarati

Table 4 Multicolor LSB Planes of Information Pixels obtained by Distributing Algorithm 2 (1 Bit LSB Insertion)

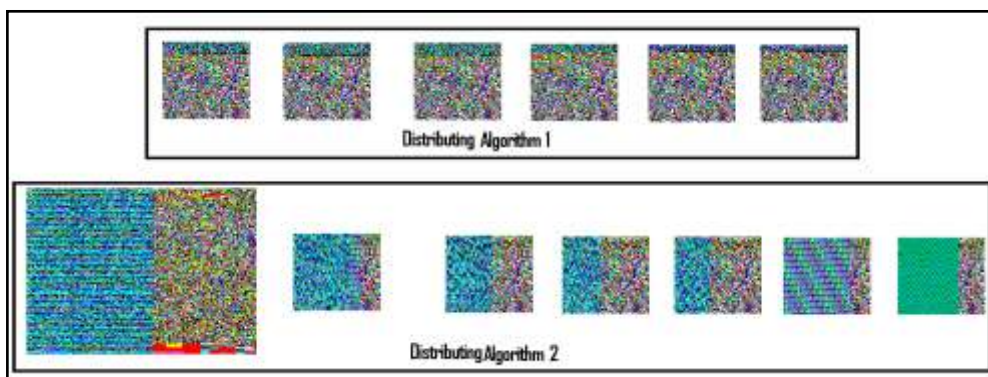


Fig 10 LSB Planes of Different Stego-Images obtained by Distributing Algorithm1 and Distributing Algorithm 2

#### IV. Conclusion

Any spatial domain steganographic algorithm either embeds the information in the Least Significant Bits of the pixel or changes the entire color code of the pixel by inserting information in more than 2 bits of the pixel. In former algorithm large number of pixels are required for inserting information because only one or two LSB is available from every pixel while in the latter algorithm the entire information can be stored in very few pixels because large number of bits are available from every pixel for storing information. Thus any spatial domain steganographic algorithm can be either Concentrating Algorithm or Distributing Algorithm. All concentrating algorithms can be easily steganalysed by Pixel Aberration Analysis of the Stego-Image as mentioned in Section 3.1. The aberration in the pixels containing information is much higher than all other pixels and therefore those few pixels with high pixel aberration can be easily identified. On the other hand Multicolored LSB Plane of any Stego Image easily reveals the presence of data in it by giving information pixels a different appearance from image pixels. This difference in appearance of Information Pixels from Image Pixels is due to unequal distribution of Red, Green and Blue Components in them. Thus the results from section 3.1 (Pixel Aberration Analysis) and section 3.2 (Multicolored LSB Plane based Analysis) clearly indicates that under both the circumstances the Spatial Domain Steganographic Algorithms can be easily steganalysed. These two approaches complement each other and together form a very strong deterrent against Spatial Domain Image Steganography. Unlike other steganalysis techniques both these approaches are very fast and consume very less computational power and at the same time not just reveal the positions of the pixels having the information but also inform the binary value of the hidden information. This binary value of the information can be easily cryptanalyzed to produce the information in human understandable form. Thus this technique can be used as a potential tool against the global terrorist networks and other cyber crime syndicates. Although this technique of steganalysis may not work directly against other innovative steganographic

algorithms (which are using techniques other than spatial domain transformation) but with appropriate improvements and modifications it can also be applied against other steganographic algorithms as well. As a foolproof approach against the Spatial Domain Steganography this technique can significantly reduce at least one arsenal in the cyber armory of terrorists and organized criminals and may make world a somewhat more safer place than it was before.

## V. Acknowledgement

I wish to sincerely thank Mr Kinjal Choudhary (Software Professional at Sapien Nitro), Shri D Praveen Kumar (DRDO Scientist at RCI Hyderabad), Lieutenant Mani Kumar, Sub Lieutenant S.S Niranjana (Engineering officers of Indian Navy) and Ms Anjala Sharma (Senior Engineer at Alstom Power) for keenly reviewing my work and for providing the necessary feedbacks for improvement of this technical paper. I am also thankful to entire staff of NCE in general and Shri DL Sapra (Senior Scientist, DRDO and Principal of NCE), Commander Mohit Kaura (Senior Engineering Officer of Indian Navy and Training Commander of NCE) and Shri Kiran Manjrekar (Scientist, DRDO and Head of Electrical) in particular for providing the necessary support and encouragement.

## References

- [1] Infosecurity Magazine article dated 02 May 2012 reports that Al-Qaeda uses Steganography to hide documents. <http://www.infosecurity-magazine.com/view/25524/alqaeda-uses-steganography-documents-hidden-in-porn-videos-found-on-memory-stick>
- [2] Daily Mail Online, UK article dated 01 May 2012 reported that a Treasure trove of Intelligence was embedded in porn video. <http://www.dailymail.co.uk/news/article-2137848/Porn-video-reveals-Al-Qaeda-plans-hijack-cruise-ships-execute-passengers.html#ixzz1uIgxpire>
- [3]. The New York Times article dated Oct 30, 2001 with title "Veiled Messages of Terror May Lurk in Cyberspace" claims 9/11 attacks planned using Steganography.
- [4] Wired article dated 02<sup>nd</sup> July, 2001 nicknamed Bin Laden as "the Steganography Master" <http://www.wired.com/politics/law/news/2001/02/41658?currentPage=all>
- [5] Kaustubh Choudhary "Image Steganography and Global Terrorism" IOSR Journal of Computer Engineering, Volum 1 Issue 2 , pp 34-48. <http://www.iosrjournals.org/journals/iosr-ice/papers/vol1-issue2/14/N0123448.pdf>
- [6] Jonathan Watkins, *Steganography - Messages Hidden in Bits (15<sup>th</sup> December, 2001)* <http://mms.ecs.soton.ac.uk/mms2002/papers/6.pdf>
- [7] Steganalysis of LSB Based Image Steganography using Spatial and Frequency Domain Features by *Hossein Malekmohamadi and Shahrokh Ghaemmaghami*
- [8] Paper titled Mathematical Modeling of Image Steganographic System by Kaustubh Choudhary (Manuscript Id: A 11264) is submitted in your esteemed journal for peer review.

## Bibliography of the Author



**Kaustubh Choudhary** Scientist, Defence Research and Development Organisation (DRDO)  
Ministry of Defence, Govt of India

### Current attachment:

Attached with Indian Navy at Naval College of Engineering, Indian Naval Ship Shivaji,  
Lonavla - 410402, Maharashtra, India