Exploiting the RGB Intensity Values to Implement a Novel Dynamic Steganography Scheme

Surbhi Gupta[1], Parvinder S. Sandhu[2]

***Abstract*—** Steganography means covered writing. It is the concealment of information within computer files. In other words, it is the Secret communication by hiding the existence of message. In this paper, we have implemented steganography in images by exploiting the properties of RGB intensity. The intensity values of R,G & B channels are categorized & then utilized for hiding message accordingly. It is completely image property based method & thus no static pattern in followed in hiding & retrieving the messages, which will make the steganalysis difficult. As the lower valued color channels are less sensitive to changes they are the main target positions for data hiding. Data hiding is performed using two channels for data hiding & one channel for indicating the existence of data in other two channels.

Keywords- Dynamic Steganography, pixel indicator technique, RGB intensity values, LSB, RGB channel.

I. INTRODUCTION

Steganography is the process of hiding a message in a medium, such as a digital picture or audio file, so as no one can even think of its presence. It is the secret transmission of a message. It is different from encryption, because the goal of encryption is to make a message difficult to read while the goal of steganography is to make a message altogether invisible. A steganographic message may also be an encrypted as an extra barrier to interception, but need not be. Used as an alternate to encryption, it takes advantage of unused bits within the file structure or bits that are mostly undetectable if modified. A steganographic message rides secretly to its destination, unlike encrypted messages, which although undecipherable without the decryption key, can be identified as encrypted. It includes a vast array of secret communication methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covered channels, and spread spectrum communications.

Data hiding requires two files. The first is the image that will hold the hidden information, called the cover image. The second file is the message- the information to be hidden. The combined image is called a stego-image or stego-file.

Ms. Surbhi Gupta is Research Scholar at Punjab Technical University, Jalandhar in the department of Computer Science Engineering. (email: royal_surbhi@yahoo.com)

Dr. Parvinder Singh Sandhu is with RBIEBT, Sahauran in the department of Computer Science. (e-mail:parvinder.sandhu@gmail.com)

When hiding information inside images the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside of is a 24 Bit jpg image as this is the largest type of file normally available & used in transmission on internet. When an image is of high quality and resolution it is a lot easier to hide and mask information inside it. Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF or JPG, the reason being is that posting of large images on the internet may arouse suspicion. It is important to remember that if you hide information inside of an image file and that file is converted to another image format, it is most likely the hidden information inside will be lost.

RGB Model

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The main purpose of the RGB color model is for the sensing, representation, and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography.

In this paper, we proposed a technique based on RGB color values. To a computer an image is an array of numbers that represent light intensities at various points (pixels) these pixels makeup the image's raster data. Digital images are typically stored in either 24-bit (RGB) or 8-bit (Grayscale) files. A 24-bit image provides the most space for hiding information; however it can be quite large (with the exception of JPEG images). All color variations for the pixels are derived from three primary colors: red, green, and blue. Each primary color is represented by one byte.

In this technique, variable numbers of bits are stored in each channel of pixel. The sequence of the channel is based on random order. Here, one channel, the first one which has a capacity of four bits, is used as a pixel indicator, that decides the state whether data is present or not in other two respective channels. Suppose if R channel acts as an indicator then G and B channels will be used to hide the data & R contains the information that whether the data is present in the channel & if it is present in last 2 or 4 bits.

II. 2. Related Work

Data hiding technique [4] is a new kind of secret communication technology. It has been a hot research topic in recent years, and it is mainly used to convey messages secretly by concealing the presence of communication. There have been proposed many techniques about data hiding. A large number of popular data hiding tools, such as S-Tools 4, HideBSeek, Steganos and StegoDos etc, that are based on LSB replacement. By using information hiding techniques, it is possible to fuse the digital content within the image signal regardless of the file format and the status of the image.

Kevin Curran [3] explained that Steganography was a process that involves hiding a message in an appropriate carrier for example an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. This was a process, which can be used for example by civil rights organizations in repressive states to communicate their message to the outside world without their own government being aware of it. Less virtuously it can be used by terrorists to communicate with one another without anyone else's knowledge. In both cases the objective was not to make it difficult to read the message as cryptography does, it was to hide the existence of the message in the first place possibly to protect the courier.

Provos and Honeyman[5] discussed existing steganographic systems and presented recent research in detecting them via statistical steganalysis. Other surveys focused on the general usage of information hiding and watermarking or else provide an overview of detection algorithms. In this paper, three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Parvez and Gutub[1] introduced a new algorithm for RGB image based steganography. This concept referred to a technique of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: lower color component stores higher number of bits. The sequence of channels was selected randomly based on a shared key. This technique ensured a minimum capacity and can accommodate to store large amount of data. Experimental results show that our algorithm performs much better compared to the existing algorithms. This algorithm can also be used to store fixed no of bits per channel, but can still offer very high capacity for cover media.

As compared to the above mentioned method our algorithm offers more capacity & robustness. Its dynamic nature makes it possible to locate the best possible positions for hiding information. In this paper, we have some experimental results showing the superiority of our algorithm and also some comparative results with other similar algorithms in image based steganography.

III. New Dynamic Algorithm

In simple LSB techniques, for every byte of an 8-bit image, one bit can be encoded to each pixel. Other methods use a static scheme for 2 bit LSB insertion in every channel & use pixel indicator channel in cyclic order making the steganalysis easier. Our technique is based on studying the RGB channel values of jpg images. It is evident that channels with low color values are less sensitive to changes in their LSB & higher color values are more sensitive to changes. We have used this property to categorize the color values in three categories. If, the color value of the channel is between 0-85, then it can afford 4 bit changes, if the value lies in between 85-170, then there will be 2 bits of changes and no data will be hidden in channels having value in between 170-255. The lower the value, the higher the data bits to be stored. So the three categories are as:

- First one which is more susceptible to changes & can accommodate 4 LSB insertions,
- Second, which accommodate 2 LSB insertion &
- Third, with no LSB insertion.

Thus this novel algorithm utilized the property of color channel to decide that whether the channel should be used for hiding information or not & that to what extent, which is the key feature of this algorithm. Moreover the pixel indicator channel is also selected randomly based on, which is the channel having a capacity of 4 bits out of R,G & B.

Our algorithm first categorizes the channels & finds out that whether the channel can afford zero, two or four bit LSB insertion. It is explained in Table I.

Then the pixel indicator channel is selected & least four bit values are encoded to hide the information regarding the rest two channels. The four least significant bits of indicator channel will be used as an indication to the existence of hidden data in other two channels as explained in Table II.

Therefore, we propose the following dynamic algorithm. The encoding process is as follows:

- Find out the capacity of each channel based on its category.
- Identify the indicator channel. The channel which is encountered first out of R, G & B & has a capacity of 4 bit insertion will be selected. The 4 LSB of indicator channel is modified as per scheme described in Table II.
- Data will be stored in one or two channels, other than pixel indicator. The capacity of channel (whether 0, 2 or 4) will be decided by its category as mentioned above.
- The image to be hidden is read channel wise, concatenated & stored in a string. A counter is set. The Relative number of bits from the string is read & the corresponding channel in the cover image is modified.
- Finally the cover image is redrawn using the new values of RGB channels to obtain the stego image.

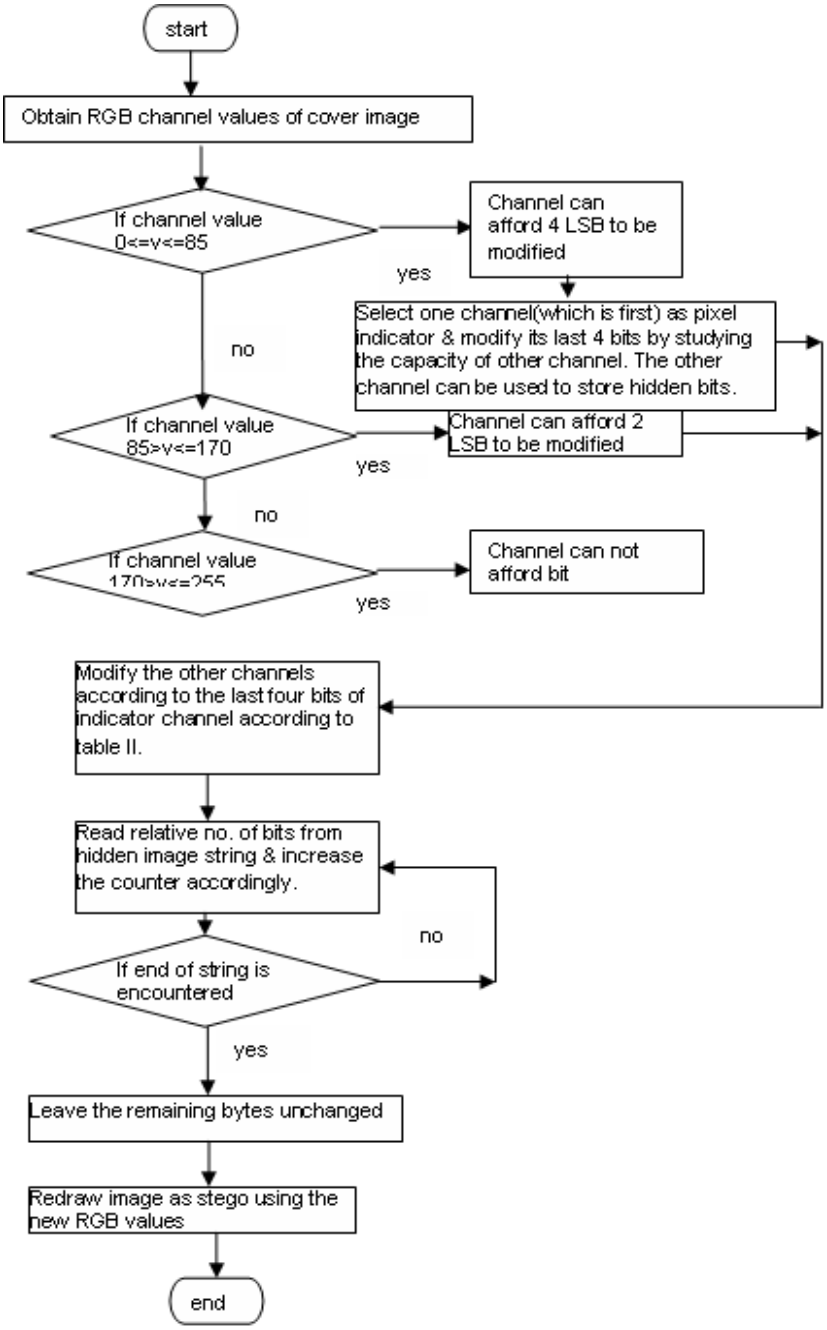

Figure1. Hiding Process

TABLE1. OUTPUT OF MATLAB PROGRAM TO INDICATE THE PREVIOUS VALUES OF RGB CHANNEL, LAST 4 BITS OF PIXEL INDICATOR CHANNEL, BITS TO BE UTILIZED IN EVERY CHANNEL & NEW CHANNEL VALUES

Old R channel values	Old G channel values	Old B channel values	4 LSB for pixel indicator channel	No of LSB bits to be modified in R channel	No of LSB bits to be modified in G channel	No of LSB bits to be modified in B channel	New R channel values	New G channel values	New B channel values
146	87	53	1100	2	2	4	147	85	60
150	92	55	1100	2	2	4	150	94	60
141	81	45	1101	2	4	4	143	93	32
137	77	41	1101	2	4	4	137	77	47
130	67	32	1101	2	4	4	131	77	39
139	77	40	1101	2	4	4	137	77	32
137	73	35	1101	2	4	4	138	77	46
156	92	54	1100	2	2	4	159	95	60
159	96	55	1100	2	2	4	159	99	60
151	88	47	1100	2	2	4	151	91	44
162	99	56	1100	2	2	4	162	96	60
165	100	58	1100	2	2	4	164	103	60
158	93	51	1100	2	2	4	156	95	60
170	106	62	1100	2	2	4	168	107	60
156	95	50	1100	2	2	4	159	95	60
157	98	54	1100	2	2	4	159	98	60
164	105	63	1100	2	2	4	167	107	60
158	99	57	1100	2	2	4	157	98	60
151	88	44	1100	2	2	4	150	91	44
159	96	52	1100	2	2	4	157	99	60
164	100	56	1100	2	2	4	164	103	60
152	89	46	1100	2	2	4	154	89	44
150	88	49	1100	2	2	4	150	90	60
150	92	54	1100	2	2	4	148	93	60
136	78	41	1101	2	4	4	138	77	35
112	59	25	1101	2	4	4	114	61	25
104	59	30	1101	2	4	4	104	61	18
83	48	26	1111	4	4	4	95	56	18
58	36	25	1111	4	4	4	63	40	25

TABLE 2. MEANING OF INDICATOR BITS WHEN REFERRING TO FOUR LEAST SIGNIFICANT BITS

Pixel indicator	Pixel(1)	Pixel(2)	Pixel(3)	Pixel(4)
0000	No hidden data	No hidden data	0-bits of data	0-bits of data
0100	No hidden data	Hidden data in 2nd channel	0-bits of data	2-bits of data
0101	No hidden data	Hidden data in 2nd channel	0-bits of data	4-bits of data
1000	Hidden data in 1st Channel	No hidden data	2-bits of data	0-bits of data
1100	Hidden data in 1st Channel	Hidden data in 2nd channel	2-bits of data	2-bits of data
1101	Hidden data in 1st Channel	Hidden data in 2nd channel	2-bits of data	4-bits of data
1010	Hidden data in 1st Channel	No hidden data	4-bits of data	0-bits of data
1110	Hidden data in 1st Channel	Hidden data in 2nd channel	4-bits of data	2-bits of data
1111	Hidden data in 1st Channel	Hidden data in 2nd channel	4-bits of data	4-bits of data

We have listed the results to prove the good quality of stego image obtained.The whole algorithm is explained in the flowchart in figure 1. This process is the hiding process. The extraction process is just the opposite, where we will extract hidden bits depending on the criteria used & redraws the hidden image. We can obtain 100% accurate image (unless the format remains same) using this scheme.

IV. CONCLUSIONS

The main features of the proposed technique are its robustness, good quality of stego image & the faithful recovery of the hidden image.
Figure 2 & 3 are the original cover image & the stego image obtained respectively. Figure 4 is the hidden image.

Figure2. Jpeg cover image, 10.7 Kb 192X144

Figure3. Stego image obtained after modifications, no differences visible from cover image

Figure4. Hidden image, 4.42 Kb, 66X66

Figure 5 & 6 are comparing the zoomed vies of original & modified image.

Figure5. Zoomed view of a subpart of original image

Figure6. Zoomed view of a subpart of modified image

Figure 7 & 8 are the 1st channel histograms of the original & the modified image. The two histogram comparison clearly proves the algorithm is statistically robust as only negligible differences are appearing.

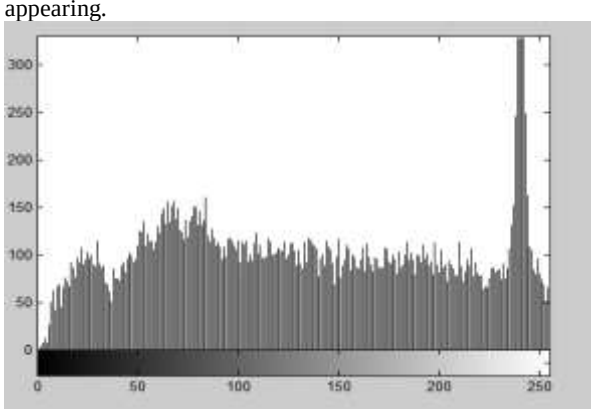

Figure7. Histogram of 1st channel of original image

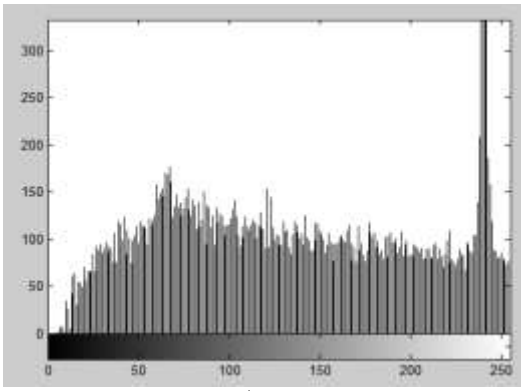

Figure8. Histogram of 1st channel of modified image

Similarly figure 9 & 10 are displaying the histograms for the 2nd channel & figure 11 & 12 are the histograms for the 3rd channel of the original & modified image.

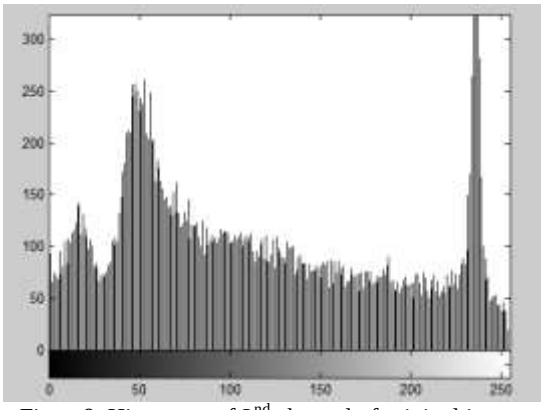

Figure9. Histogram of 2nd channel of original image

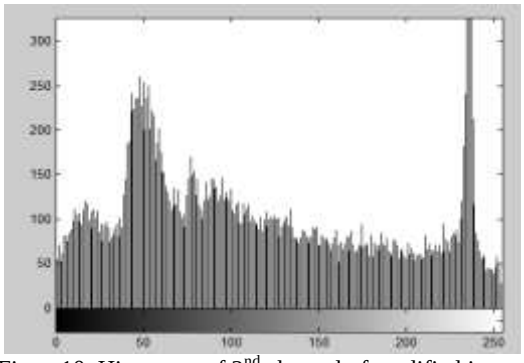

Figure10. Histogram of 2nd channel of modified image

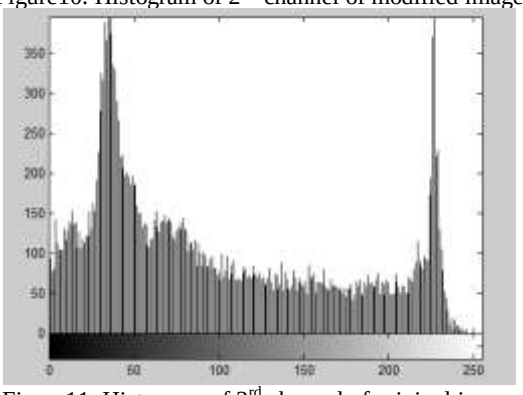

Figure11. Histogram of 3rd channel of original image

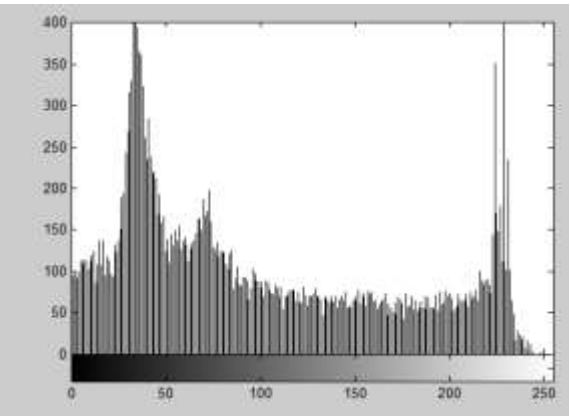

Figure12. Histogram of 3rd channel of modified image

FUTURE WORK

The proposed algorithm is implemented using the ideal RGB color model. The same algorithm can be implemented in other color models as YCbCr or L*a*b to further exploit its advantages. Further more features of such models can be used to find out the possible targets for data hiding without affecting the quality of image.

REFERENCES

[1] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh "Triple-A: Secure RGB Image Steganography Based on Randomization" aiccsa, pp.400-403, 2009 IEEE/ACS International Conference on Computer Systems and Applications, Rabat, Morocco May 10- 13, 2009

[2] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, *Pixel indicator high capacity technique for RGB image based Steganography*, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications,University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008

[3] Karen Bailey, Kevin Curran, An evaluation of image based steganography methods using visual inspection *and automated detection techniques*, Multimedia Tools and Applications, Vol 30 , Issue 1 (2006) pp. 55-88

[4] N.F. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, 31(2)(1998) 26-34

[5] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, 01 (3)(2003)32-44

[6] Mohammad Tanvir Parvez and Adnan Gutub, "RGB Intensity Based Variable-Bits Image Steganography", APSCC 2008 – Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12 December 2008.