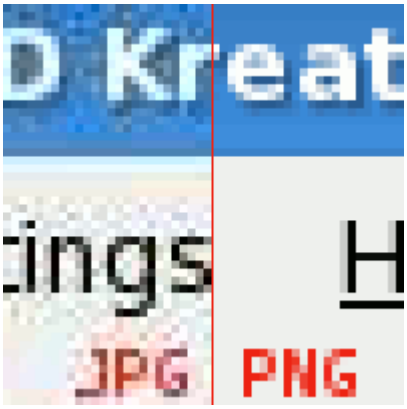

Figure 1: Zoomed Images (image source: Google)

2.2.1. Joint Photographic Expert Group (JPEG)

The most well-known format i.e. JPEGis an abbreviation for "Joint Photographic Experts Group," which is also the name of the committee that developed this popular image format. JPEG is a compressed image file format. JPEG images consist of a huge array of colors which makes it the best choice for compressing photographic images. It is a highly popular format thus, you will come across it many times in your day to day life. Though JPEG images are high resolution images which has high color depth and clarity, it is a lossy format, which means some quality is lost when the image is compressed. After each compression the image losses its original form and thus, after a certain amount of compression the image completely loses its integrity and appears as block of colors just like lego pieces.

(a) Properties of JPEG

- Popular format for all imaging devices.
- Compressed format.
- This format allow a wide range 8-24 bits indexed color.
- Uses lossy compression algorithms.

2.2.2. Portable Network Graphics (PNG)

PNG which stands for Portable Network Graphics is very popular image format used over the internet. This format was developed to overcome the drawbacks of GIF file formats [4]. It supports palette based images i.e. 24 bits for RGB and 32 bits for ARGB where A stands for alpha channel of the image. This was specifically designed for internet usage thus, does not support other color model apart from RGB. It provides lossless compression, thus providing real image after every compression.

(a) Properties of PNG

- Popular format for usage over the internet.
- Lossless Compression Algorithms are used.
- Only RGB model applicable.
- Provides 24 or 32 bit depth for images.

Table 1: Comparison of JPEG and PNG

	JPEG	*PNG*
File Type	Joint Photographic Expert Group	Portable Network Graphics
File Suffix	.jpg	.png
File Size	small	Larger than JPEG
Resolution	High	High
Support Color	16 Million Colors	Much Higher in 32 bit
Complexity	Quite Complex	Comparatively Simpler
Ideal For	Camera	Internet
Color Depth	8-24 bits	24-32 bit
Compression Algorithm	Lossy	Lossless

3. Steganography in JPEG

Theimage-based steganography are broadly divided into two categories:

- Frequency domain Steganography
- Spatial domain steganography.

The first digital image steganography was done in the spatial domain using LSB coding (replacing the least significant bit or bits with embedded data bits) [16]. JPEG transforms spatial data into the frequency domain [3]and employs a lossy compression thus, on each processing and then conversion back to spatial domain, the image loses its integrity due to introduction of too much noise and loss of data. These would be hard to correct using error correction coding. Hence, it was concluded that steganography would not be possible in JPEG images.JPEG encoding is divided into lossy and lossless stages [14]. DCT transformations to the frequency domain and quantization stages are lossy, whereas entropy encoding of the quantized DCT coefficients (which we will call the JPEG coefficients to distinguish them from the raw frequency domain coefficients) is lossless compression [3] and researchers took advantage of this property of JPEG and decided to embed data bits inside the JPEG coefficients before the entropy coding stage.

4. An overview of LSB

A digital image is a 2 Dimensional array of varying intensity levels. For gray scale image, 8 bits per pixel are used whereas in a color image following RGB model, there are 24 bits/pixel, 8 bits assigned to each color components. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [5]. The LSB uses a simple concept of replacing the last bit with the message bit. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [9]. For example a grid for 3 pixels of a 24-bit image can be as follows: (00101101 00011100 11011100) (10100110 11000100 00001100) (11010010 10101101 01100011) When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows: (00101101 00011101 11011100) (10100110 11000101 00001100) (11010010 10101100 01100011) Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [10]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [5]. The advantage of LSB embedding is its ease and many techniques use these methods [5]. But, if the

security aspect is considered it may not be a good choice dueto its low robustness and tamper resistance. They are highly sensitive to any sort of image processing like cropping, filters, resizing, contrasting etc.

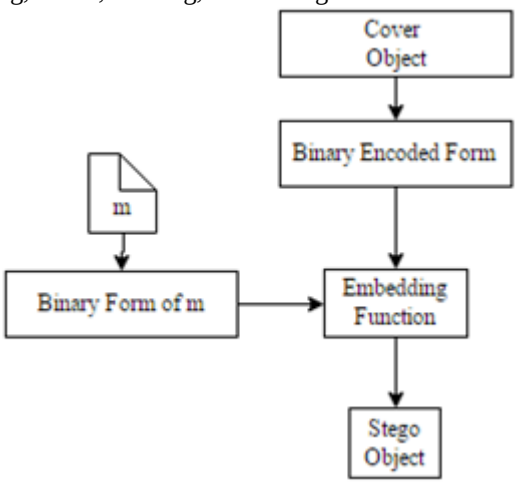

Figure 2: Basic Flow of LSB Steganography Process

4.1. Advantages of LSB

1. LSB algorithm is it is quick and easy to implement.
2. Causes minimal distortion per unit area of image.
3. LSB insertion also works well with gray-scale images

4.2. Disadvantages of LSB

1. Low robustness.
2. Highly vulnerable to cropping, contrasting and other sort of image processing.

4.3. The LSB Algorithm

1. Select cover-object CO as an input.
2. Encode the CO in binary [12].
3. The Secret Message, m.
4. Encode the m in binary [12].
5. Choose one pixel of the CO randomly.
6. Use a pixel selection to hide information in the CO.
7. Save the new image (Stego-object) SO in the desired format.

4.4. LSB in PNG image format

PNG format for a LSB Steganography is a great choice. As the LSB works on spatial domain thus, it becomes very important that there is no introduction of noise or error of any sort. Under this scenario PNG is the best format due to the fact that it uses a lossless compression so the substitutions made during the whole process of LSB steganography is not lost. PNG also provides huge storing capacity and high quality image after steganography thus, avoiding detection by just looking at the image.

4.5. LSB in JPEG image format

For a JPEG image, LSB is similar to what is done in LSB for PNG with a slight difference that they are entropy encoded after embedding of bits.

LSB embedding [13], [14], and [15] is the most common technique to embed message bits DCT coefficients. This method has also been used in the spatial domain where the least significant bit value of a pixel is substituted with the message bits. It is done by associating an even coefficient with a zero bit and an odd one with a one. In order to embed a message bit in a pixel or a DCT coefficient, the sender increases or decreases the value of the coefficient/pixel to embed a zero or a one. The receiver then extracts the hidden message bits by reading the coefficients in the same sequence. And decoding them in accordance with the encoding technique performed on it. LSB embedding in JPEG images offers good embedding capacity and low visual detection by human eye. It provides capacity of almost one bit per coefficients using the frequency domain technique.

5. Application and Evaluation

5.1 Images before Steganography

Figure 3(a):JPEG Figure 3(b): PNG

Figure 4(a): JPEG Figure 4(b): PNG

Table 2: Description of Images used

Name	*JPEG(a)*			*PNG(b)*		
	Size MB	*Dimension X*Y*	*Depth BPP*	*Size MB*	*Dimension X*Y*	*Depth BPP*
Fig 3	5.08	5616x3744	24	27.9	5616x3744	24
Fig 4	0.4	1920x1080	24	3.33	1920x1080	24

5.2. Images after Steganography

Figure 5(a): JPEG **Figure 5(b):** PNG

Figure 6(a): JPEG **Figure 6(b):** PNG

Table 3: Comparison of LSB for JPEG and PNG

	PNG	*JPEG*
Efficiency on reasonable data	High	Medium
Data Capacity	Medium	Low
Detection (Steganalysis)	Medium	Medium
Resultant Image Distortion	Medium	Medium
Robustness against Image Manipulation	Medium	Medium
Robustness against statistical attack	Medium	High
Payload Capacity	Medium	Medium
Independent File Format	Low	Low
Suspicion on the basis of File created	Low	Low
Visibility	Low	Low

6. Conclusion

It was observed that conventional LSB is not effective in case of JPEG as the data gets manipulated on compression due to its lossy nature. Whereas for a PNG image a simple LSB is applicable without any loss of data on compression. Also, they both fair almost equal in terms of storing capacity and image quality of final image.

References

[1] "Steganography", http://en.wikipedia.org/wiki/Steganography
[2] Henk C. A. van Tilborg (Ed.), "Encyclopedia of cryptography and security", pp.159. Springer (2005).
[3] Eltyeb E. A bed Elgabar,"Comparison of LSB Steganography in BMP and JPEG Images", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013
[4] "Portable Network Grapics", http://en.wikipedia.org/wiki/Portable_Network_Graphics
[5] Johnson, N.F. &Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal,February 1998.
[6] Hemalatha.S, U.Dinesh Acharya and Renuka.A, (2013) "Comparison of Secure and High CapacityColor Image Steganography Techniques in RGB and YCBCR domains", International Journal ofAdvanced Information Technology, Vol.3, No.3,
[7] C.P.Sumathi, T.Santanam and G.Umamaheswari," A Study of Various Steganographic TechniquesUsed for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013
[8] "An Introduction to PNG", http://www.libpng.org/pub/png/book/chapter01.html
[9] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.
[10] NXP & Security Innovation Encryption for ARM MCUs ppt.
[11] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002.
[12] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 391
[13] D. Llamas, C. Allison, and A. Miller, \Covert channels in internet protocols: A survey," in Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, 2005.
[14] Neil R. Bennett, JPEG STEGANALYSIS & TCP/IP STEGANOGRAPHY, University of Rhode Island, 2009.
[15] H. Wu, N. Wu, C. Tsai, and M. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proceedings-Vision, Image and Signal Processing, vol. 152, no. 5, pp. 611–615, 2005.
[16] W. Pennebaker and J. Mitchell, JPEG still image data compression standard. Kluwer Academic Publishers, 1993.

Author Profile

Bharat Sinhais student of Galgotias college of Engg. & Tech. and is pursuing his B.Tech in Computer Science & Engineering 2015 Batch.