ADVANCED STEGANOGRAPHIC TECHNIQUE FOR BOTH COLORED AND GRAY-SCALE IMAGES

GunjanVerma[1], Shailendra Singh[2],Vipin[3], Md Shamsul Haq[4]

[1,4] Department of MCA, MIET, Meerut, (India)

[2,3] Department of CSE, MIET, Meerut, (India)

ABSTRACT

The internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. It is important to reduce the chances of the information being detected during the transmission. This is an important issue now-a- days. Thus, there must be some solution to solve the problem, so as to pass information in a manner that the very existence of the message is unknown to third person or attacker in order to repel attention of the potential attacker. This paper defines the various techniques used for information hiding, their applications and also discusses the drawbacks of implementing those techniques independently. The motivation for this paper includes provision of protection of information during transmission without any detection of information. In the present work, it has been observed that steganography is the solution for given problem as in this technique, existence of data is not evident. Among various types of steganographic techniques, image steganography is best solution. In the past few years a large number of algorithms for image steganography have been developed n order to have better imperceptibility, a mathematical method 2^k correction has been used. This method corrects each pixel-value as 2^k. This means if k-bits are embedded in a pixel value the method adds or subtracts 2^k to each pixel-value and finally the corrected pixel value becomes closer to the original-pixel. Hence, the secret data in the stego-pixel is not changed.

Keywords*: *First Component Alteration Technique Interception Steganography, Stego-Pixel, Vulnerable.

I. INTRODUCTION

1.1. Information Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms information security, computer security and information assurance are being used frequently interchangeably. However, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used and the areas of concentration. Information security is concerned with the **confidentiality, integrity and availability of data** regardless of the form the data may take electronic, print or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. The field of information security offers many areas for specialization including: securing

networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc. Three basic principles of information security are shown in fig 1.1

Fig. 1: Information Security

II. INFORMATION HIDING TECHNIQUE

The introduction of the various processes of the last decades have continuously pointed out towards the security requirement levels, especially since the massive utilization of personal computers, networks and the internet with its availability. Many techniques have been developed for avoiding theft of data, controlling quantities of possible copies. These techniques used for data hiding are:

- **Cryptography**
- **Digital Watermarking**
- **Steganography**

III. STEGANOGRAPHY

In this paper we use the steganography technique to secure the information or data.The word steganography comes from Greek word "steganos" meaning "covered" and the "graphy" means "writing". Thus, steganography literally means "covered writing".Steganography is a very old method of passing messages in secret. This method of message cloaking goes back to the time of the ancient Greeks. The historian Herodotus [4] has written about how an agent wrote a message warning of an invasion on the wood part of a wax tablet. Since, messages were normally inscribed in the wax and not the wood, the tablet appeared blank to a common observer

IV. PRINCIPLES OF STEGANOGRAPHY

Computer steganography is based on two principles:

1. The digitized images or sound can be altered to a certain extent without causing any noticeable effect on them so as to hide the data in them.
2. The human inability to distinguish minor changes in image color or sound quality, with which one can easily hide the data, be it 16 bit sound, 8 bit or even better 24-bit image. Speaking of image, changing the value of first component of pixel of an image wouldn't result in any detectable change of that color.

4.1 Different Kinds of Steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 2 shows the four main categories of file formats that can be used for Steganography.

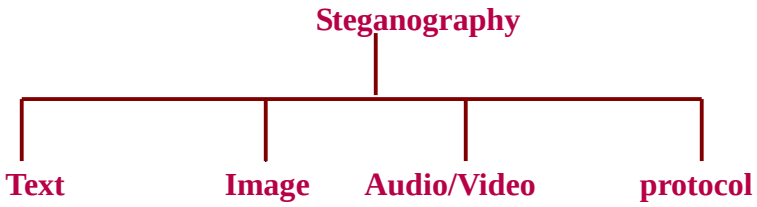

Fig. 2: Categories of Steganography

Text steganography using digital files is not used very often since text files have a very small amount of redundant data. Given the proliferation of digital images, especially on the internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography. In this paper, an image steganographic technique has been proposed.

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound.

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

4.2 Basics of Embedding

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 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. Steganography, strives for high security and capacity, which often entails that the hidden Information is fragile. Even trivial modifications to the stego medium can destroy it. A classical steganographic system's security relies on the encoding system's secrecy.

V. IMAGE QUALITY PARAMETERS

Image quality parameters are figures of merit used for the evaluation of imaging system or processes. The image quality parameters can be broadly classified into two categories **[6]**, subjective image quality and objective image quality. Subjective image quality is a method of evaluation of images by the viewers and it emphatically examines fidelity and at the same time considers image intelligibility. In the objective measures of the image quality metrics, some statistical indices are calculated to indicate the reconstructed image quality. The image quality parameters provide some measures of the closeness between two digital images by exploiting the differences in the statistical distribution of pixel values. The most commonly used quality parameters for comparing stego image and original image are:

- Mean Square Error (MSE),
- Peak Signal to Noise Ratio (PSNR),
- Root Mean Square Error (RMSE)

5.1. Mean Square Error (MSE)

The mean of pixel values of the image and by averaging the sum of squares of the error between two images.

$$\text{MSE} = \frac{1}{M*N}\sum_{x=1}^{M}\sum_{y=1}^{N}[x(m,n) - y(m,n)]^2$$

Where x (m, n) and y (m, n) are the two images of size M*N. In this case x is the original image and y is the stego image.

The lower the value of Mean Square Error (MSE) signifies lesser error in the stego image.

5.2. Peak Signal to Noise Ratio (PSNR)

The Peak Signal to Noise Ratio (PSNR) measures the estimates of the quality of stego image compared with an original image and is a standard (benchmark) way to measure image reliability or conformity.

$$\text{PSNR} = 20log_{10}[\frac{\text{MAXPIX}}{\text{RMSE}}]$$

Where MAXPIX is the maximum pixel value and RMSE is the Root Mean Square Error of the image (it quantifies the average sum of distortion in each pixel of the stego image i.e. average change in pixel caused by encoding algorithm)

$$\text{RMSE} = \sqrt{MSE}$$

In PSNR 'signal' is the original image and 'noise' is the error in the stego image resulting due to encoding and decoding. PSNR is a number that reflects the quality of the stego image and is measured in decibel (dB).

Also Mathematically:

Peak Signal to Noise Ratio (PSNR) is inversely proportional to the Mean Square Error (MSE), which implies the

lower the value of Mean Square Error (MSE) higher is its Peak Signal to Noise Ratio (PSNR). Thus higher the Peak Signal to Noise Ratio (PSNR) is better.

VI. INTRODUCTION TO FIRST COMPONENT ALTERATION TECHNIQUE

From the literature surveyed, we get that there is a strong need to improve quality of stego image so that stego object and cover object looks same. A new scheme called first component alteration technique has been proposed which improves quality of stego image and gives better results then **J.G. Yu's [1]** method.

The scheme is based on following principle:

The matrix of pixels represents every image. According to the basic RGB color model, every pixel is represented by the three bytes namely red, green and blue. The significance of these colors is as follows:

Red: Gives the intensity of red color in that pixel

Green: Gives the intensity of green color in that pixel

Blue: Gives the intensity of blue color in that pixel

According to Hecht **[5],** the human eye is less sensitive to blue color. Therefore, first or blue component of pixel has been used to store one byte of information as it doesn't effect color value of the pixel. This way the secret messages are stored inside the image to form stego image and this stego image is sent to the destination. At the receiving end, characters from the pixels of stego image are extracted and the message is reconstructed from the image. The method is tested by well known parameters namely PSNR and RMSE. It has been observed that the MSE value is decreased and PSNR value is increased. Thus image quality is improved.

A new image steganographic technique is presented with improved quality parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). The proposed scheme can encode any image files (JPEG, BMP, DIF) having 24 bits per pixel in order to protect confidential text data from unauthorized access. The technique has low computational complexity, so can be applied to very small images (24 X 24) as well as large images (512 X 512). In this technique, 8 bits of first component of pixel have been replaced with secret bits of text data. The results show that quality parameter values of PSNR are much higher than all the previous existing image steganographic techniques.

VII. DESCRIPTION OF FIRST COMPONENT ALTERATION TECHNIQUE

Techniques used so far focuses only on the two or four bits of a pixel in a image, (at most five bits at the edge of an image) which results in less peak to signal noise ratio and high root mean square error i.e. less than 45 PSNR value. The research work concentrated on 8 bits of a pixel (8 bits of blue component of a 24 bits pixel in an image), resulting better image quality.

In a computer, images are represented as arrays of values. These values represent the intensities of the three colors R(ed), G(reen) and B(lue), where a value for each of the three colors describes a pixel. Figure 3 shows an image containing group of pixels. According to RGB model, a pixel contains three color components that are red, green

and blue component.

In this technique, sender and receiver should know common stego key. This stego key is used by receiver to extract secret message from stego image sent by sender to him. Sender selects an image called cover image or original image in which he wants to hide the secret message. Image containing the secret data is called stego image. Now, in this method, the bits of first component (blue component) of pixels have been replaced by key and secret message. Firstly key is converted into binary form and its binary form is filled in the first component of first pixels. After then, secret message is converted into binary form and its binary form is filled in first component of next pixels. Blue channel is selected because a research was conducted by Hecht **[5],** which reveals that the visual perception of intensely blue objects is less distinct than the perception of objects of red and green. Figure 4 shows 24 bit size pixel. In this pixel, Blue layer in a pixel have been replaced with data embedded blue layer.

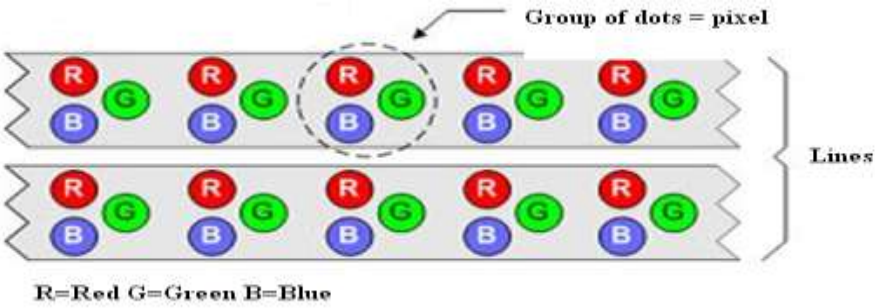

Fig. 3: Image containing Group of Pixels

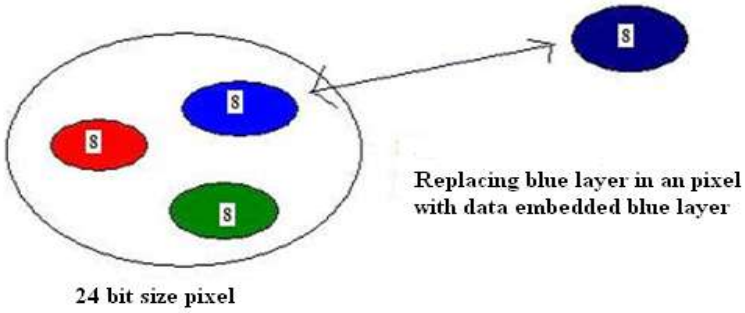

Fig. 4: Replacement of Blue Layer with Data Embedded Blue Layer

7.1. First Component Alteration Technique Example

One can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are:

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

A steganographic program could hide the letter "A" which has a position 65 into ASCII character set and have a binary representation "01000001", by altering the blue channel bits of pixels and key be the letter “C” which has a position 67 into ASCII character set and have a binary representation "01000011".

(01000011 11101001 11001000) (01000001 11001000 11101000)

(11001000 00100111 11101001)

VIII. PSNR AND MSE FOR COLORED AS WELL AS GRAY-SCALE IMAGES

The results are obtained in tabular form for above images using PSNR calculator tool. The values of PSNR and MSE and the comparison between PSNR and MSE for above images are shown in Table 1 and in Figure 6.1 respectively.

Table. 1: Different PSNR and MSE Values

Image	Size	PSNR(dB)	MSE
Lena(C)	512 × 512	47.94	1.056
Niagra(C)	375 × 512	47.95	1.054
Airport(C)	400 × 318	47.96	1.052
Lena(G)	400 × 300	47.93	1.057
Building(G)	500 × 486	47.94	1.057

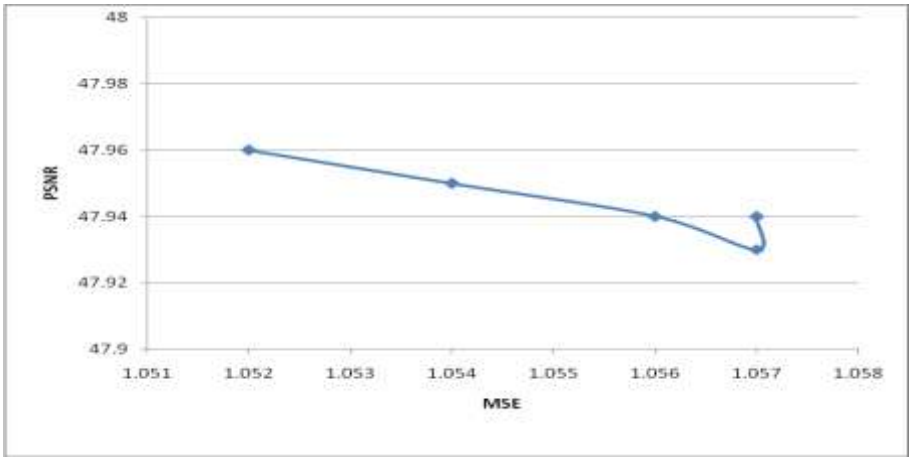

Fig. 5: Different PSNR and MSE Values

IX. PSNR AND MSE OF R-G-B COLOR PATTERNS FOR COLORED AS WELL AS GRAY-SCALE IMAGES

The results and analysis of R-G-B color patterns are shown is Table 2 and the graphical comparison is shown in three graphs Figure 6, 7 and 8 for Red, Green and Blue (R-G-B) color patterns respectively.

Image	Size	PSNR(R)	PSNR(G)	PSNR(B)	MSE(R)	MSE(G)	MSE(B)
Lena(C)	512 × 512	47.37	47.53	48.92	1.188	1.148	0.832
Niagra(C)	375 × 500	47.39	47.54	48.92	1.185	1.145	0.832

Baboon(C)	400 × 318	47.39	47.54	48.93	1.183	1.143	0.831
Lena(G)	400 × 300	47.37	47.52	48.92	1.190	1.149	0.833
Building(G)	500 × 486	47.36	47.53	48.93	1.191	1.148	0.835

Table. 2: Different PSNR and MSE values for R-G-B Color Patterns

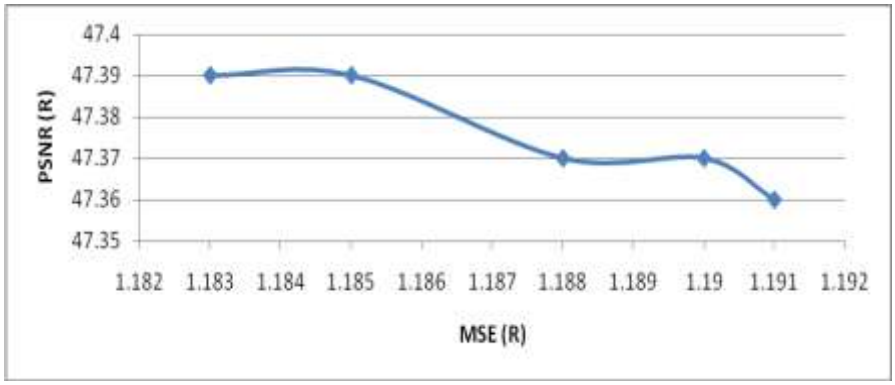

Fig. 6 : Different PSNR and MSE Values for RED Color Pattern

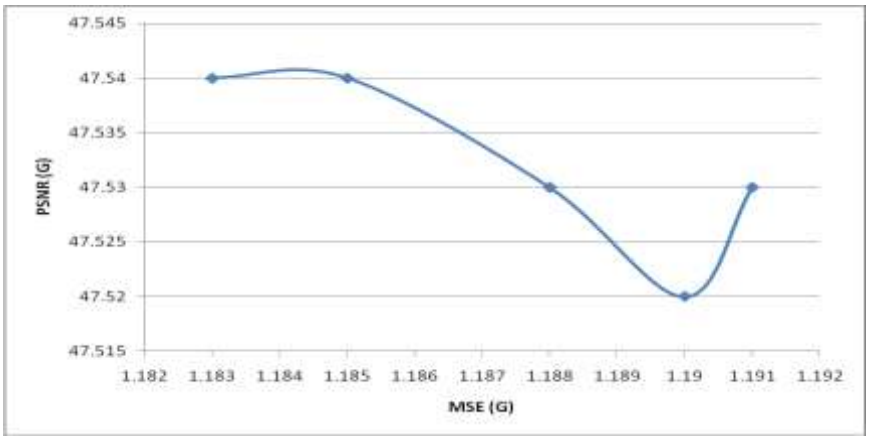

Fig. 7: Different PSNR and MSE Values for GREEN Color Pattern

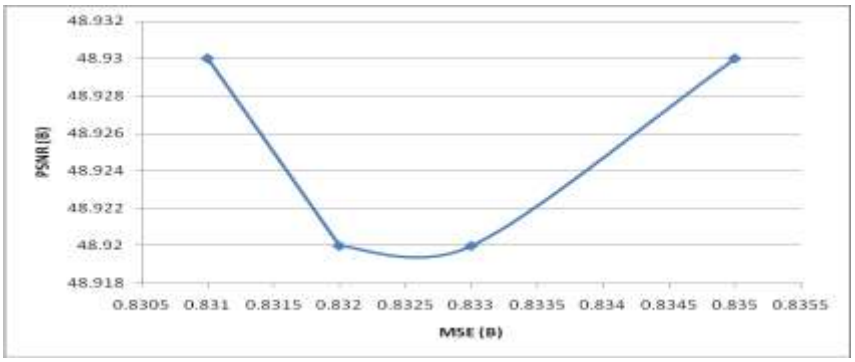

Fig. 8: Different PSNR and MSE Values for BLUE Color Pattern

X. CONCLUSION

A new first component alteration technique for image encoding and decoding has been presented .The proposed scheme can encode any image files (JPEG, BMP or DIF) having 24 bits per pixel in order to protect confidential data from unauthorized access. The algorithm has low computational complexity, can be applied to very small images (24 × 24) as well as large images (512 × 512).

The results and analysis of the proposed techniques are shown above. We have compared the PSNR and MSE of whole resolution of the image as well as compared the PSNR and MSE of R-G-B color patterns separately.

XI ACKNOWLEDGEMENT

Our thanks to the experts and authors and referenced journals who have contributed towards development of the paper and help us for making the concepts clear.

REFERENCES

[1] J.G. Yu, E.J. Yoon, S.H. Shin and K.Y. Yoo, "A New Image Steganography Based on 2^k Correction and Edge-Detection," In Fifth International Conference on Information Technology: New Generations, pp. 563-568, 2008

[2] Y. H. Yu, C. C. Chang and Y. C. Hu, "Hiding Secret Data in Images via Predictive Coding," Pattern Recognition, vol. 38, pp. 691-705, 2005.

[3] C.Y. Yang, "Color Image Steganography based on Module Substitutions," In Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, vol. 2, pp.118-121, 2007.

[4] Y.R. Park, H.H. Kang, S.U. Shin and K.R. Kwon, "A Steganographic Scheme in Digital Images Using Information of Neighboring Pixels," In International Conference on Natural Computation, pp. 962-967, 2005.

[5] E. Hecht, Optics, 2nd Ed, Addison Wesley, 1987

[6] W. Stallings, "Cryptography and Network Security: Principles and Practice," Prentice- Hall, New Jersey, 1999

[7] J.R. Smith and C. Dodge, "Developments in Steganography", In Proceedings of the Third International Information Hiding Workshop, vol. 1768, pp. 77-87, 1999.

[8] J. Cummins, P. Diskin, S. Lau and R. Parlett, "Steganography and Digital Watermarking,"www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/ SS5/Steganography.pdf, 2004.

[9] M. Niimi, H. Noda and E. Kawaguch, "An image embedding in image by a complexity based region segmentation method," in Proceedings of the 1997 International Conference on Image Processing (ICIP '97), pp. 74, 1997.

[10] Y.K. Lee and L.H. Chen, "High capacity image steganographic model", IEE Proc. Vision Image Signal Process, vol. 147, pp. 288-294, June 2000.