Volume 3, No. 3, March 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

# AN ADAPTIVE STEGANOGRAPHY TECHNIQUE FOR GRAY AND COLORED IMAGES

Sherish Johri[1] and Amit Asthana[2]
[1]IMS Engineering College, Ghaziabad, UP, India.
[2]Subharti Institute of Technology & Engineering, Meerut, India.
sherish3@gmail.com,
amitasthana80@gmail.com

***Abstract:*** In recent years, Steganography and Steganalysis are two important areas of research that involve a number of applications. These two areas of research are important especially when reliable and secure information exchange is required. Steganography involves embedding of message into a cover media and hides its existence. On the other hand Steganalysis is the technology that attempts to defeat Steganography by detecting the hidden information and extracting. So for the maintenance of secrecy either we need to make more robust steganography techniques against steganalysis or discover new and better techniques. In this paper, we propose a novel and more robust image steganography technique that embeds message into a cover media and hides its existence and can verify the reliability of the information being transmitted to the receiver. In order to hide secret data in cover-image it used the Image and Text files representation in Array, that takes the alteration component based approach and method of Palette Based Images. The bits of encrypted message will be hidden inside the stretched palette of image.

***Keywords:*** Steganography techniques; Information Hiding; Information Security; Alteration based approach; Palette based image.

## INTRODUCTION

Generally, the information may be becomes secret by using two techniques that's broadly used for security purposes [3], such as cryptography and steganography. The methods of cryptography render the data unintelligible to outsiders by various transformations, whereas the methods of steganography conceal the existence of messages. Steganography perform two principles, the first one is the capacity of hidden secret data, and another is the quality of the stego image. Steganography is a way for secret communication by using digital media to convey essential messages; it is the art and science of hiding communication. Thus it embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion [27]. The most common thing in Steganography is to use images for steganography. This is called image steganography, in which the pixels of images are changed in order to hide the secret data so as not to be visible to users [10]. Also, watermarking used for privacy and copy right protection, [4] in field of data security

Images are the most popular cover objects used for steganography. The digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist. This numeric representation forms a grid and the individual points are referred to as pixels [29]. Most images on the internet consists of a rectangular map of the image's pixels (represented as bits). Not surprisingly the larger amount of colors that can be displayed, the larger the file size.

The word steganography comes from the Greek Steganos, which means covered or secret i.e., Steganography means literally covered writing. It is the method of hiding information such that its presence cannot be detected [1], such that an adversary is supposed to be unable to distinguish between cover and stego images. A secret message is embedded in such a manner that the existence of the information is hidden and to establish a secured communication in a completely undetectable manner [2]. In the case of images, the carrier is referred to as the cover image, while after embedding secret data into it; the stego image can be obtained.

Different types of security techniques are used for providing security are as follows:
Spread Spectrum techniques, ables to hides data are spread throughout the cover-image making it harder to detect [31]. Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies [32]. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image.

JPEG Steganography is one which hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be destroyed. However, properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs. One of these properties of JPEG is exploited to make the changes to the image invisible to the human eye. During the DCT transformation phase of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable [30].

File Structure Based Steganographic Methods Different image file formats have different header file structures. The secret information can be hidden not only in the data values, e.g., pixels, palette, DCT coefficients, but also in the header structure or at the end of a file [28]. For instance, Invisible Secrets and Steganozorus hide data with the comment fields in the header of JPEG images. Camouflage, JPEGX, PGE10 and PGE20 add data at the end of a JPEG image.

The information vulnerable to unauthorised access and interception, while in storage or transmission. The threat of an intruder and Steganalysis accessing secret information for sharing information over an unsecure or covert communication channels are vulnerable to intruder attacks. Although, these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media that minimizes the threat of intrusion. Therefore, to maintain secrecy either we need to make more robust steganography techniques against steganalysis or discover new and better techniques.

This paper organized in Parts. Firstly we describe the introduction of Security of data, Steganography, Images, and other security Techniques under the heads of Introduction in Part-I. Subsequently we have gone through the literature review and found problems and solutions in several papers. All this we have mentioned under heads of Backgrounds in Part-II. In Part-III, the proposed architecture and mechanism described in detail. Finally, this paper concluded and mentions its further enhancements under future scope in Part – IV and Part-V respectively. All used references used during writing of this paper are mention in Part –VI under head of references.

## BACKGROUNDS

A novel steganographic method [5] based on JPEG [19]. It takes advantage of the quantization error resulting from processing the JPEG-compressed image [21, 22] with two different scaling factors. One of the scaling factors is used to control the bit rate of the stego image while the other is used to guarantee the quality of the stego image. Experimental results show that this steganographic method provides high information hiding capacity and successfully control the compression ratio and distortion of the stego image.

A color image steganography method based on the module substitutions [6] is proposed. In accordance with the base-value of the blocks, a variety of secret bits is embedded to a RGB trichromatic system by three types of module substitutions [23]. More specifically, to alleviate further color distortion and obtain a larger hidden capacity, the R-, G- and B-component is encoded by Mod u, Mod u-v, and Mod u-v-w substitution, respectively. Experiments show that both PSNR and hiding rate generated by this method are better than those generated by the reported schemes. In addition, the resulting perceptual quality is good.

A least significant bit [8] (4LSB) is a substitution method [12, 13]. The 4LSB method is implemented for color bitmap images (24 bit and 8 bit i.e. 256 color palette images) and wave files as the carrier media. When applying 4LSB techniques to each bytes of a 8-bit image, one bit can be encoded to each pixel. Any changes in the pixel bits are indiscernible to the human eye. By using this algorithm, one can hide its file of any format in an image and audio file. He can then send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, can open the file, extract the secret information and decrypt it.

An image steganograph [9] gives high capacity and good security. Based on local complexity of a cover image, varying-depth embedding is used to improve the imperceptibility and to decrease distortions in it. Experimental results show that the steganographic technique provides higher capacity and be resistant to several well-known steganalytic methods.

New image steganography scheme which is a kind of spatial domain technique [10]. In order to hide secret data in cover-image, author used the Just Noticeable Difference (JND) technique and method of Contrast Sensitivity Function (CSF) [24, 25]. This is an edge-detection which uses part information of each pixel-value. In order to have better imperceptibility, a mathematical method 2k correction is proposed. 2k correction corrects each pixel-value as 2k. This means if *k*-bits are embedded in a pixel value, the method adds or subtracts 2k 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. This scheme embeds more data than previous schemes and shows better imperceptibility.

Secure Image Steganography based on Randomized Sequence of Cipher Bits [16] provides a technique based on seed ranking. In order to hide image it uses single image for suitability based on seed ranking. It does not require the user to select the multiple images for suitability. Steganography when combined with randomized sequence of cipher bits provides a better means of secret communication between two parties. This application is based on seed ranking of an image.

## PROPOSED STEGANOGRAPHY TECHNIQUE

### *Architecture of Proposed Steganography Technique: Sender's View:*

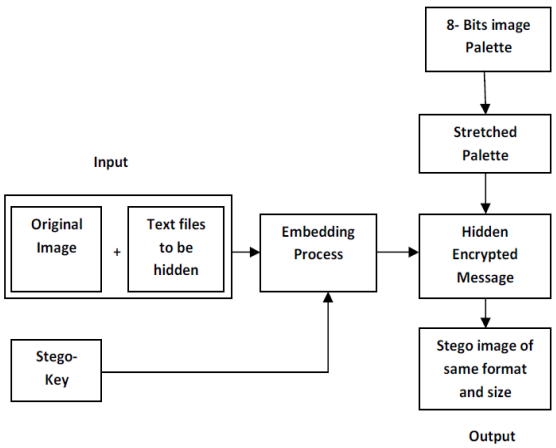


Figure – 1: Sender's View of Steganography Techniques.

Figure-1 shows the sender's view of Steganography Technique in which sender Input an image called cover image or original image of any file format(JPEG, BMP,DIP etc ) in which he wants to hide the secret message and text file containing secret data has to be embedded in an image file. Image containing the secret data is called stego image. Next phase is to select the stego key for encoding. In Embedding process data is hidden by using Alteration component technique in which 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. For more security of stego image Palette Based Images technique is applied by stretching process. Finally, the output is obtained of same format and size that gives better result in form of than existing techniques.

***Receiver's View:***

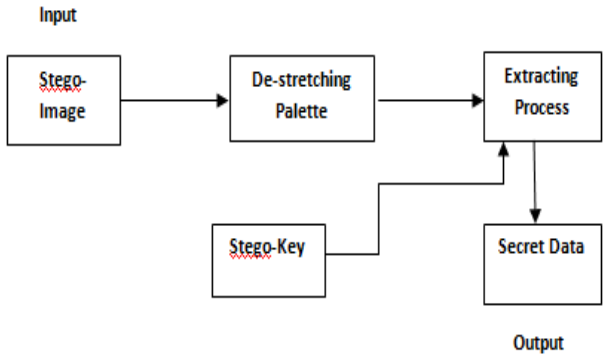


Figure – 2: Receiver's View of Steganography Technique.

Figure-2 shows the receiver's view of Steganography Technique in which the sender sends a stego-image to the receiver. The receiver having the stego key to extract secret data from stego image. The receiver must have the same key with which the image is embedded. On Stego image De-stretching Palette pocess is applied by using Extracting process which is Alteration Component techniques. Finally we get the Secret Data which is embedded.

***Mechanism of Proposed Steganography Technique:***

***Sender's View (Encoding):***

***Phase 1: Original Image and Text File:*** The original image is of any file format having 24 bits per pixel. Due to low computational complexity, it can be applied to very small images (24 x 24) as well as large images (512 X 512). This technique can encode gray scale images as well as colored images directly, with R-G-B levels. After selecting image file, text file is selected which contains secret data.

***Phase 2:*** Stego Key Variable key called stego key is selected for security purpose. Both sender and receiver knows same stego key. If the key is valid, then only receiver can decode image and retrieve secret data

***Phase 3:*** Embedment of Data and Stego Key in Image using Alteration Technique and Palette Based Images

**Step (a):** Fetch all the pixels of the given image and fix it in the corresponding space i.e. F (i,j).

**Step (b):** Fetch all the characters of the given text file and fix it in corresponding space i.e**.** K (i,j).

**Step (c):** Fetch all the characters from the Stego key and fix it in the corresponding space i.e**.** L (i,j).

**Step (d):** Choose first pixel and pick characters from L (i,j) and place it in first component of pixel. If there are more characters in L (i,j), then place rest in the first component of next pixels, otherwise follow Step (e).

**Step (e):** Place some identification symbol to indicate end of the key, "0" has been used as a identification symbol in this algorithm.

**Step (f):** Place characters from K (i,j) in each first component (blue channel) of next pixels by replacing it.

**Step (g):** Follow step (f) till all the characters has been embedded.

**Step (h):** Again place some identification symbol to indicate end of data.

**Step (i):** Now stretched the palette (look-up table) of obtained image.

**Step (j):** Obtained image will hide all the characters that we input.

***Receiver's View (Decoding):***

**Phase - 1: Stego Image:** The sender sends a stego image to the receiver. The receiver is having the stego key to decode secret data from stego image.

**Phase - 2:** Stego Key after receiving stego image by receiver or legitimate user, the legitimate user must have the same shared key with which the image is encoded.

**Phase - 3:** Extracting of Stego Image using Proposed Alteration Component and Palette based Image Technique:

Decoding algorithm includes following steps:

**Step (a):** First of all de- stretch the palette (look-up table) of the stego-image.

**Step (b):** Consider three arrays. F(i, j), L(i,j) and K(i,j).

**Step (c):** Extract all the pixels in the given image and store it in the array called F (i, j).

**Step (d):** Now, start scanning pixels from first pixel and extract key characters from first (blue) component of the pixels and place it in Key-Array L(i,j). Follow Step 3 till we get terminating symbol, otherwise follow step (e).

**Step (e):** If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program by displaying message ―Key is not matching.

**Step (f):** If the key is valid, then again start scanning next pixels and extract secret message characters from first (blue) component of next pixels and place it in Character Array c(i,j). Follow Step (f) till we get terminating symbol, otherwise follow step 6.

**Step (h):** Extract secret message from K(i,j). Thus in this way secret message is decoded and received by receiver.

## CONCLUSION

It was appeared that [10,11,13,14] uses 4LSB techniques which was not able to store tremendous information and

even not more secure. This paper proposed a novel image steganography technique that work on 8LSB techniques and could embed more data than related previous steganography schemes by hiding secret data in cover-image. It used the Image and Text files representation in Array, that takes the alteration technique based approach and method of palette by stretching process. Not only does this scheme hides more data and has better imperceptibility than others available techniques but also has improves quality of stego image and gives better results than existing one.

## FUTURE ASPECTS

The proposed steganography technique for gray and colored images will provide effective security for images with efficient manner but this work may be further improved for other types of images like TIFF, JPEG2000 etc .Video files can also be used to transmit data, however the time consumption will increase in this case.

## REFERENCES


[1]. C. Cachin, "An Information-Theoretic Model for Steganography", In 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.

[2]. R Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", In IEEE pp. 1019-1022, 2001

[3]. W. Stallings. Cryptography and Network Security – principles and practices. Pearson Education, Inc., 2003.

[4]. L. A. Bygrave, "The technologisation of copyright: implications for privacy and related interests," European Intellectual Property Review, vol. 24, no. 2, pp. 51–57, 2002.

[5]. H.W. Tseng and C.C. Chang, "Steganography Using JPEG-Compressed Images," In Fourth International Conference on Computer and Information Technology, pp. 12-17, 2004.

[6]. 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.

[7]. Steganography and the Art of hiding information by Vish Krishnan, Overland Park, K.S.

[8]. S .K. Moon and R.S. Kawitkar, "Data Security using Data Hiding," International Conference on Computational Intelligence and Multimedia Applications, vol. 4, pp. 247-251, 2007.

[9]. J. He, S. Tang and T. Wu, "An Adaptive Image Steganography Based on Depth-Varying Embedding," In Congress on Image and Signal Processing, vol. 5, pp. 660-663, 27-30 May 2008.

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

[11]. W. N. Lie and L. C. Chang." Data hiding in images with adaptive number of least significant bits based on the human visual system." *Proc. ICIP '99*, 1:286–290, 1999

[12]. H. T. S. M. Kharrazi and N. Memon. "Image Steganography: Concepts and Practice". WSPC, 2004.

[13]. Alkhraisat Habes, "Information transmissions in computer network. Information hiding in bmp image Implementation analysis and evaluation" (Jan.2006)

[14]. S. K. Moon, V. N. Vasnik, "Application of steganography on image file", National conference on Recent trends in Electronics, pp. 179-185

[15]. Chns J Mitchell " The Institution of Electrical Engineers Printed and published by the IEE". Savoy Place, London WC2R OBL, UK, 1995.

[16]. AKL Subba Rao Y.V , Brahmananda Rao S.S , Rukma Rekha N, " Secure Image Steganography based on Randomized Sequence of Cipher Bits", Eighth International Conference on Information Technology: New Generations, 2011.

[17]. Rabah, K "Steganography : The Art of Hiding Data" Information Technology Journal ,Vol 3 No.3, pp. 245-269, 2004.

[18]. Kessler, G. "An Overview of Steganography for the Computer Forensics Examiner ", Computer & Digital Forensics Program, Champlain College, Burlington, Vermont, February 2004

[19]. W. Pennebaker, J. Mitchell, "JPEG Still Image Data Compression Standard". Van Nostrand Reinhold, New York, 1993.

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

[21]. H. Kobayashi, Y. Noguchi, H. Kiya, "Method of Embedding Binary Data into JPEG Bitstreams," IEICE Trans. Information and Systems, vol. J83-D, no. 2, 1999, pp. 1469- 1476.

[22]. N. Johnson, S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software," Proceedings of Information Hiding Workshop, Portland, Oregon, USA, Apr. 1998, LNCS 1525, pp. 273-289.

[23]. Y.Y Tsai, and C.M. Wang, "A novel data hiding scheme for color images using a BSP tree," The J. of Sys. and Software 80, 2006, pp. 429-437.

[24]. A. J. M. W. Osberger and D. McLean. A computational model of the human visual system for image quality assessment 1997.

[25]. T. N. Pappas and R. J. Safranek. Handbook of Image and Video Processing. Academic Press, 1999.

[26]. Pan ,H.K., Y.Y., Chen, and Y.C., Tseng, "A Secure Data Hiding Scheme for Two-Color Images", Proc. Fifth IEEE Symp. Computers and Comm., IEEE Press, Piscataway, N.J., 2000.

[27]. P. H. N. Provos. "Hide and seek: An introduction to steganography". IEEE Security and Privacy, 1(3):32–44, 2003.

[28]. Y. O. Yildiz, K. Panetta and S. S. Agaian, "New quantization matrices for JPEG steganography," Proceedings of SPIE, vol. 6579, pp. 65790D- 1–65790D-11, 2007.

[29]. "Reference guide: Graphics Technical Options and Decisions", http://www.devx.com/projectcool/Article/1997


 

[30]. Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998

[31]. Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis" , Communications of the ACM, 47:10, October 2004

[32]. Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[33]. S.G.K.D.N. Samaratunge, "New Steganography Technique for Palette Based Images," In Second International Conference on Industrial and Information Systems, pp. 335-340, Aug. 8 – 11, 2007.

**Short Bio Data for the Author**

**Sherish Johri** is working as Assistant Professor in IMS Engineering College, Ghaziabad (U.P). He has been in teaching for more than four years. He has been member of several academic and administrative bodies. During his teaching he has coordinated several Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national and international conferences. His area of research includes Network Security, ERP and Data Mining

Amit Asthana is working as Assistant Professor in Subharti Institute of Technology & Engineering at Subharti University, Meerut (U.P.). He is persuing his Phd from Subharti University, Meerut. He has been in teaching for more than five years. He has supervised more than 5 students M.Tech. dissertation. He has been member of several academic and administrative bodies. During his teaching he has coordinated several Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national and international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).

 