Steganography using the Technique of Orderly Changing of Pixel Components

Madhu Bahl
Astt. Prof.
CEC Landran,
Mohali, India

Akshay Girdhar
Assoc. Prof.
Guru Nanak Dev Engineering College,Ludhiana,
India

ABSTRACT
A new proposed scheme is presented for digital image steganography which is a kind of spatial domain technique, works with the orderly replacement of the pixel components with the text data that is to be embedded . Proposed work is concentrated on 8 bits of a pixel (8 bits of Red or Green or blue component of a pixel in a 24 bit image), resulting better image quality. The proposed scheme shows higher PSNR and lower MSE than those generated by the reported schemes. To prove this scheme, several experiments are performed and compared the experimental results with the related previous works [6].

Keywords
Steganography, Stego image, Cover image, Peak Signal to Noise Ratio, Mean Square Error.

1. INTRODUCTION
The rapid development of the Internet and the digital information revolution caused significant changes in the global society, ranging from the influence on the world economy to the way people nowadays communicate. Broadband internet connections and almost an errorless transmission of data, facilitate people to distribute large multimedia files and make identical digital copies of them. These first-view advantages of digital media over the analogue ones transform to disadvantages with respect to the intellectual rights management due to the possibility for unlimited copying without a loss of fidelity cause a considerable financial loss for copyright holders. The ease of content modification and a perfect reproduction in digital domain have promote the protection of intellectual ownership and the prevention of the unauthorized tampering of multimedia data to become an important technological and research issue . To protect the copyright of the owner and safeguard the intellectual property right of ownership, people often use data hiding techniques to achieve the goals [10].

Steganography has been proposed as a new, alternative method of data hiding. Steganography as it often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Steganography is defined as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication" [10]. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. In a digital world, Steganography and cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security [2].

Image steganographic techniques can be divided into two groups [3, 9]: the Spatial Domain technique group, and the Transform Domain technique group. The Spatial domain technique embeds information in the intensity of the pixels directly, while the Transform domain technique embeds information in frequency domain of previously transformed image. Our proposed scheme is a kind of the spatial domain techniques. The rest of the paper is organized as follows. The review of previous work done is briefly specified in Section 2. The proposed technique of steganography along with the procedures of the encoding part and decoding part of the proposed method are also included in Section 3. Experimental results are demonstrated in Section 4. Finally, a conclusion is summarized in Section 5.

2. PREVIOUS WORK
Several steganography techniques have been proposed. The most commonly approaches modify the least significant bits (LSB) of an image based on the assumption that least significant bits are insignificant. This method is probably the easiest way of hiding information in an image. But by using this method on average only half of the LSB's will be modified so having less data hiding capacity[7,8,13].

The Steganographic technique has to possess two important properties. These are good imperceptibility and sufficient data capacity. A new scheme which satisfied both properties based on first component alteration was proposed. This new technique of steganography is simple and has a higher embedding capacity than other schemes. In a computer, images are represented as arrays of values [6]. These values represent the intensities of the three colors R (Red), G (Green) and B (Blue), where a value for each of three colors describes a pixel. Each pixel is combination of three components(R, G, and B). In this scheme, the bits of first component (blue component) of pixels of image have been replaced with data bits, which are applied only when valid key is used. Blue channel is selected as a research was conducted by Hecht, which reveals that the visual perception of intensely blue objects is less distinct that the perception of objects of red and green. For example, suppose 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.

(**01000001** 11101001 11001000) (00100111 11001000 11101000) (11001000 00100111 11101001)

This technique has high embedding capacity about overall bright images and has high distortion of a cover image when the embedding is done only on the blue channel of a pixel.

3. PROPOSED IMAGE STEGANOGRAPHY SCHEME

In the proposed scheme, a new steganography scheme based on spatial domain technique is introduced. More specifically, to alleviate further color distortion and to achieve better PSNR and lower MSE than first component alteration method ,the steganography based on orderly changing of pixel components is proposed. In this scheme, the 8-bits of first component of first pixel is replaced with first character of secret data then second component of second pixel is replaced with second character of secret data then third component of third pixel is replaced with third character of secret data and repeat this process for other character of secret data by choosing next order set of the pixel from pixel array till all the characters of secret data has been embedded.

For example, suppose 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 text X, Y, Z which has a position 88, 89, 90 respectively into ASCII character set and have a binary representation 01011000, 01011001, 01011010", by altering the blue channel bits of pixels.

(00100111 11101001 **01011000**) (00100111 **01011001** 11101001) (**01011010** 00100111 11101001)

3.1 Embedding Phase

The embedding process is as follows:

Inputs: Image file and the text file

Output: Text embedded image

Procedure:

Step 1: Extract all the pixels in the given image and store it in the array called Pixel-Array

Step 2: Extract all the characters in the given text file and store it in the array called Character-Array.

Step3: Extract all the characters from the Stego key and store it in the array called Key-Array.

Step 4: Choose first pixel and choose first order and place the key character in first component of the first Pixel.

Step 5: Choose second pixel and choose second order and place the key character in second component of the second Pixel.

Step 6: Choose third pixel and choose third order and place the key character in third component of the Third Pixel.

Step 7: Repeat Step 4, 5, 6 for other character of the key by choosing next order set of the pixel from pixel array till all the characters of key-array has been embedded

Step 8: Place some terminating symbol to indicate end of the key. '0' has been used as a terminating symbol in this algorithm.

Step 9: Orderly place characters of Character- Array in component of next pixels (i.e. first in by replacing it till all the characters has been embedded.

Step 10: Again place some terminating symbol to indicate end of data.

Step 11: Obtained image will hide all the characters that are input to it.

The flowchart to graphically represent the steps of embedding phase of proposed algorithm is shown in fig. 1.

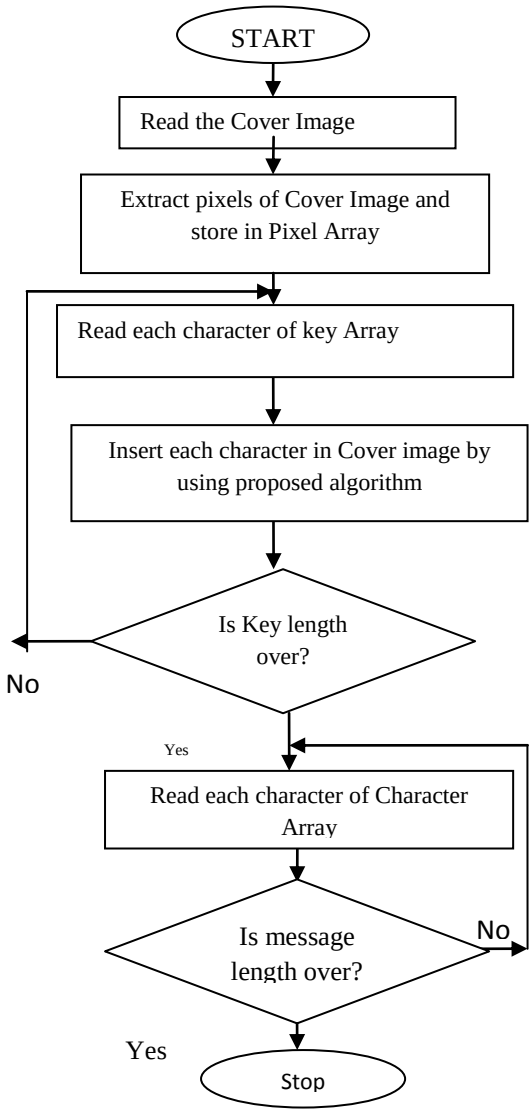


Fig. 1. Flowchart of Embedding Phase

3.1 Extracting Phase

The extracting process is as follows

Input: Embedded image file

Output: Secret text message

Procedure:

Step 1: Consider three arrays. Let they be Character-Array, Key-Array and Pixel-Array.

Step 2: Extract all the pixels in the given image and store it in the array called Pixel-Array.

Step 3: Now, start scanning pixels from first pixel and extract key characters orderly from first, second and third order

component of the pixels and place it in Key-Array till the terminating symbol, otherwise follow step 4.

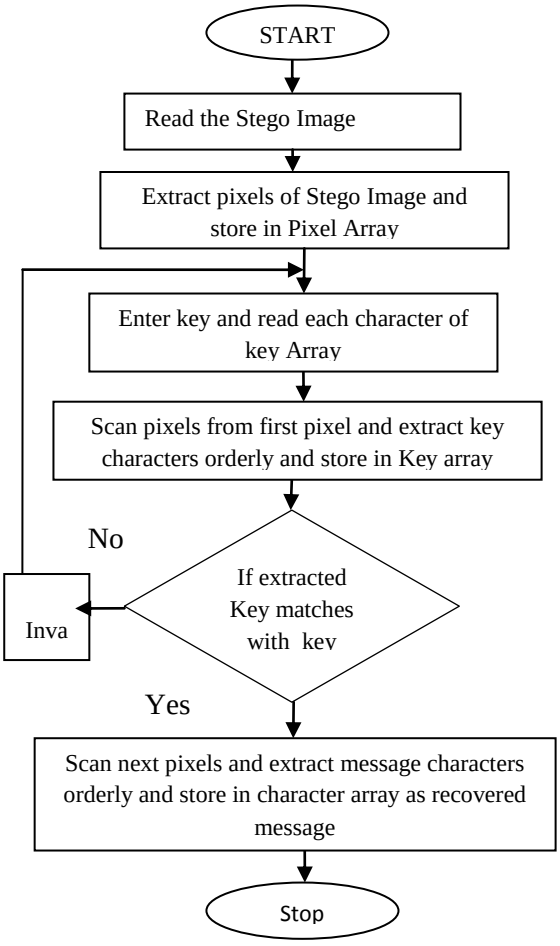
Step 4: If this extracted key match with the key entered by the receiver, then follow Step 5, otherwise terminate the program by displaying message "Key is not matching".

Step 5: If the key is valid, then again start scanning next pixels and extract secret message characters from first, second and third order component of next pixels orderly and place it in Character Array. Follow Step 5 till the terminating symbol, otherwise follow step6.

Step 6: Extract secret message from Character-Array.

The flowchart to graphically represent the steps of embedding phase of proposed algorithm is shown in fig. 2.

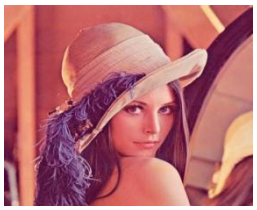
Fig.2 Flowchart of Extracting Phase



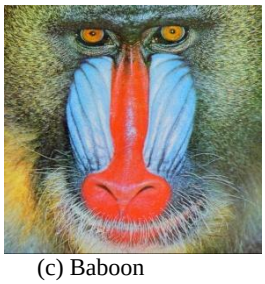
4. EXPERIMENTAL RESULTS

Different results have been observed with RGB components by replacing pixel component to embed data in it. To measure image quality of the proposed scheme, Peak Signal-to-Noise Ratio (PSNR) is used and the MSE (Mean Square Error) for an stego Image. The results are then compared with the First component Alteration technique as shown in the table. The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and stego image. The higher the PSNR, the better the quality of the stego image. The MSE (Mean Square Error) represents the cumulative squared error between the compressed and the original image, the lower the value of MSE, the lower the error. Four images, namely, Airplane, Ship, Baboon and Parachute shown in Fig. 3 were used as host images. Each RGB pixel of the host images is represented by 24 bits, 8 bits per component. These images were also used as the test images during the simulations. The mixed images generated by the proposed method are depicted in Fig. 4. It is depicted that the perceived quality of the mixed images is good. The PSNR for the R-, G-, B-component in each mixed image are also listed in Table 1. A color image steganography scheme gracefully presented by Kaur et al. [6] Was used to compare with the proposed method. The PSNR and MSE of both techniques is tabulated in Table 2. It is clear that the average PSNR generated by the proposed method are superior to those generated by First Component Alteration method.

(a) Airplane



(b) Lena



(c) Baboon

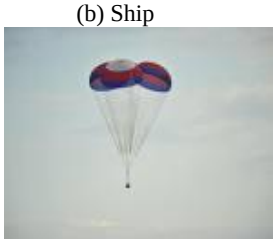
(d) Ship

Fig. 3. The four host images. (a) Airplane,(b) Lena, (c) Baboon, and (d) Ship.

(a) Airplane

(b) Ship

(c) Missile



(d) Parachute

Fig. 4. The four stego images generated by proposed technique

Stego	Peak Signal to Noise Ratio/Mean Square Error			Average	Average
images	R-Plan	G-Plan	B-Plan	PSNR	MSE
Airplane	45.91/1.665	48.92/ 0.833	47.21/1 .234	47.35	1.244
Ship	46.02/ 1.624	48.95/ 0.826	47.28/ 1.21	47.42	1.221
Missile	45.92/ 1.624	48.92 /0.832	47.22/ 1.23	47.36	1.241
Parachute	45.91/ 1.664	48.92/ .833	47.21/ .233	47.35	1.243

Table 1. PSNR and hiding rate generated by the proposed method on each R-, G-, and B-plane of the stego images.

Stego Images	First Component Alteration Method	Proposed Method
Airplane	46.10/1.727	47.35/1.244
Ship	46.16/1.697	47.42/1.221
Missile	46.11/1.723	47.36/1.241
Parachute	46.10/1.725	47.35/1.243

Table 2. Performance comparison between First Component Alteration method [6] and the proposed method.

5. Conclusion

A new image steganography scheme is presented which is a kind of spatial domain technique. The proposed method uses orderly replacement of pixel components with the secret data i.e. the 8-bits of first component of first pixel is replaced with first character of secret data then second component of second pixel is replaced with second character of secret data then third component of third pixel is replaced with third character of secret data and repeat this process for other character of secret data by choosing next order set of the pixel from pixel array till all the characters of secret data has been embedded .Simulations show that the PSNR and MSE for the proposed method outperform those for the reported schemes. Since the resulting perceptual quality of the mixed images is good, it is hardly attracted from eavesdropper by naked eye. With a good hidden capability, the proposed method can also be used as a space-saving tool for hiding private data.

6. ACKNOWLEDGMENTS

The constant guidance and encouragement received from **Mr. Akshay Girdhar**, Assistant Professor, Department of Information Technology, GNDEC Ludhiana has been of great help in carrying our the present work and is acknowledged with reverential thanks.

7. REFERENCES

[1] Anderson, R. and Kuhn, M., "Information Hiding - A Survey", *Proceedings of IEEE Conference IEEE International Conference* (IEEE, 1999), pp. 1062-1078.

[2] Caldwell,J., "Steganography", Software Engineering Technology, pp.25-27 (2003).

[3] Chen, Chen,M.,Agaian,S. and Chen,C.,"Generalized Collage Steganography on Images" *Proceedings of IEEE International Conference* (IEEE,2008), pp.1043-1047.

[4] Cummins, J. Diskin, Patrick and Parlett, R.,School of Computer Science, The University of Birmingham, "Steganography and Digital Watermarking" (2004).

[5] Johnson, N. and Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Proceedings of IEEE International Conference on Computing Practices* (IEEE, 1999), pp. 26-34.

[6] Kaur,A.,Dhir,R. and Sikka,G.,"A New Steganography Based on First Component Alteration Technique", *International Journal of Computer Science and Information Security* (IJCSIS,2009) , pp. 53-56 .

[7] Lie, W. and Chang, W.," Data hiding in images with adaptive number of least significant bits based on the human visual system", *Proceedings of IEEE International Conference*, (IEEE, 1999), pp. 286–290.

[8] Moon, S. and Kawitkar, R.,"Data Security using Data Hiding", *Proceedings of IEEE International Conference on Computational Intelligence and Multimedia Applications,* (IEEE, 2007), pp.247-251.

[9] Swanson, M. and Zhu, B., "Robust Data Hiding for Images", *IEEE Digital Signal Processing Workshop* (IEEE, 1996), pp. 37-40.

[10] *Thampi, S.,"Information Hiding Techniques: A Tutorial Review", ISTE-STTP onNetwork Security & Cryptography, LBSCE (2004).*

[11] *Yang, C.,"Color Image Steganography based on Module Substitutions", Third International Conference on International Information Hiding and Multimedia Signal Processing (IEEE,2007), pp.118-121.*

[12] *Yu1, J. Yoon2, E. and Yoo, K.," A New Image Steganography Based on 2k Correction and Edge-Detection", ITNG Proceedings of the Fifth International Conference on Information Technology: New Generations (IEEE,2008), pp.563-568.*

[13] *H.-C. Wu, N.-I. and Hwang, M.-S.," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", Proceedings of IEEE International Conference on Vis. Image Signal Process., (IEEE,2005) pp. 611-615.*