High Level of Perceptibility and Security in Color Image Steganography

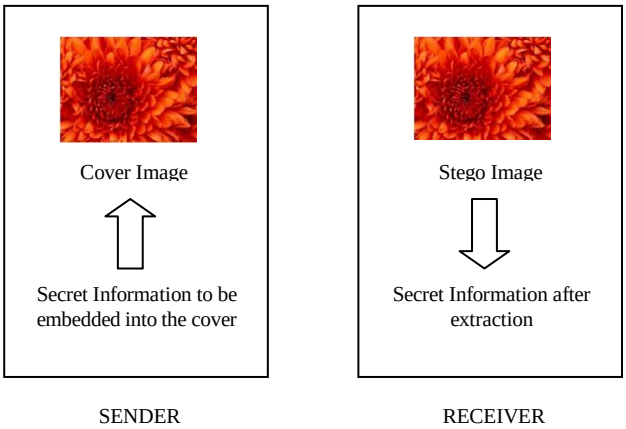
Soumen Bhowmik, Aditi Ghosh, Arup Kumar Bhaumik

***Abstract*— This paper proposes a new steganography technique to keep the quality of the cover image and increase the security. To improve the capacity of the amount of data to be embedded yields perceptible degradation of stego-image. The proposed research work is based on the color image steganography in spatial domain with maximum data capacity. Using this method the perceptible quality degradation will be minimized and security will be enhanced.**

***Index Terms* — cover image, indicator, steg-analysis, embedding, steganography, cryptography.**

I. INTRODUCTION

Steganography is an approach of hiding some valuable information into other digital media in such a way that other than the concerned people will not get any clue regarding the concealed message into the carrier media. The word "steganography" is basically of Greek origin which means "hidden writing". The word is divided into two parts: "steganos" which means secret and "graphic" which means writing. Steganography [1] is used to hide secret messages or images [2] into other media such as image, text, sound or video. The advantage of steganography is that it hides information in an imperceptible way, so the intruder will not get any clue regarding the concealed messages.



***Soumen Bhowmik**, Assistant Professor, CSE Department, Bengal Institute of Technology and Management, Santiniketan, Phone/ Mobile No.09832157090, India.*

***Aditi Ghosh**, M. Tech Student, CSE Department, Bengal Institute of Technology and Management, Santiniketan, India, Phone/ Mobile No.08017586544.*

***Prof. (Dr.) Arup Kumar Bhaumik**, Principal, RCCIIT, Kolkata, Mobile No. 09007030104, India.*

The most popular technique of steganography is embedding a message into a color image using LSB technique [3], [10], [14] In this method the data is being hidden in the least significant bit of each pixel component in the cover image. Binary representation of the hidden data is taken and it is replaced at the LSB of each byte within the cover image. There is a lack of security in the LSB technique which can be further enhanced by the proposed steganographic technique in spatial domain.

II. LITERATURE SURVEY

Internet is essential and fastest media for communication in the modern era. In data communication, it is susceptible to face many problems such as copyright protection, hacking, eavesdropping etc. and for this; security in communication is highly appreciable. Cryptography, watermarking and steganography are the different techniques for data security. Some of the existing image steganography approaches are:

LSB technique [3], [10], [11] is the simplest among all other existing image steganographic technique in spatial domain. Applying LSB technique to each byte of a 24-bit image, maximum three bits can be encoded into each pixel, as each pixel is represented by three bytes. In case of a 8-bit image, only one bit can be encoded into each pixel as each pixel is represented by one byte.

PVD [4], [9] stands for Pixel Value Differencing. In this technique, the difference between two consecutive pixel i.e. (p_i, p_{i+1}) is determined first i.e. $d_i = | p_i - p_{i+1} |$. After that, a range table is searched to find out in which range the difference d_i falls. Based on the range length, one can identify the number of bits to be embedded in each pixel. If the range length is L, then $\log_2 L$ bits are to be embedded in each pixel. Consequently, the two pixel values are modified in such a way that the difference between these two pixel values is equal to the new difference. After finding the range length, we can find how many numbers of bits should be embedded in each pixel. If the range length is L, then we can embed $\log_2 L$ bits in each pixel. For example, if the range length is 16, then 4 bits will be embedded.

In the year 2007, Singh et al. [5] proposed a better steganogrphic technique for embedding secret messages into the edges [12] of the cover image. It has introduced a new least significant bit embedding algorithm for hiding secret messages in non-adjacent pixel locations at the edges of images. Here the messages were hidden in regions which were least like their neighbouring pixels i.e. regions that contain edges, corners, thin lines etc so that an attacker will

ISSN: 2278 – 7798 All Rights Reserved © 2016 IJSETR

have less suspicion of the presence of message bits in edges, because pixels in edges of an image appears to be much brighter or dimmer than their neighbours. Edges can be detected by edge detection filters such as a 3x3 window Laplacian edge detector. One common disadvantage of LSB embedding was that it created an imbalance between the neighbouring pixels. Here this imbalance was avoided by flipping the gray-scale values among 2i-1, 2i and 2i+1. The various strengths of this scheme were that an attacker will have less suspicion to the presence of message bits in edges because pixels in edges appear to be either much brighter or dimmer than their neighbours and it was also secure against blind steganalysis. It also limits the length of the secret message to be embedded. The main disadvantage with this scheme was that the embedding capacity was relatively low. It could not make full use of edges during embedding.

In the year 2008, Zeng et al. [6] proposed a new adaptive least-significant bit (LSB) steganographic method based on pixel-value differencing (PVD) [13]. The difference value of two consecutive pixels estimates how many secret bits to be embedded into the two pixels. Pixels located in the edge areas were embedded with more secret bits than that located in smooth areas. The range of difference values were adaptively divided into lower level, middle level, and higher level. The readjusting phase ensures that the two consecutive pixels belong to the same level both before and after embedding. The range [0, 255] of difference values was divided into different levels. For extracting data exactly, the difference values before and after embedding must belong to the same level. This scheme provides more capacity and better quality than the PVD and was an improved version of PVD. The main disadvantage with this scheme was that it was less tolerant to steganalysis.

In 2011, Ghosal [7] proposed a novel steganographic technique which is initially based on the computation of number of 1's and number of 0's in the Red component of the first pixel. Then, the absolute difference between this two is calculated and is divided by 2. Hence, the resultant numbers of bits are embedded in other two channels (Green and Blue). Here, the Red component will act as an indicator. For example, take the value of the Red, Green, Blue components as: R(11011011), G(01101101), B(10101111). In R, the number of 1's and 0's are 6 and 2, respectively. Their absolute difference is (6-2) = 4 which yields 2 bits of data embedding in G and 2 bits of data embedding in B. Simulation results of this technique ensured that the embedding capacity of this technique is more than the other four techniques discussed so far. However, the problem of this technique is that when the number of 1's and 0's are equal then no bits will be embedded in that pixel.

The pixel indicator technique is proposed by Gutub [8] which uses one component of a pixel as the indicator component whereas the other two components are used to hide the secret data. According to this technique, two least significant bits of the indicator channel is checked. If these two bits are 00, then in channel 1 and channel 2, there will be no insertion of hidden data. If it is 01, then 2 bits of the hidden data will be embedded in channel 2 however, in channel1 there will be no embedding. If it is 10, then 2 bits of the hidden data will be embedded in channel 1 only. In channel 2 there will be no embedding. If it is 11, then in both channel, 2 bits of the secret data will be embedded. This technique will be more secure if for the first pixel, the RED channel will act as an indicator channel, for the second pixel the GREEN channel will act as an indicator, for the third pixel the BLUE channel will act as an indicator and so on. When RED channel is an indicator, channel 1 and channel 2 will be GREEN and BLUE respectively. When GREEN channel is an indicator, RED channel will be channel 1 and BLUE channel will be channel 2. If BLUE channel is an indicator, RED channel will be channel 1 and GREEN channel will be channel 2. The advantage of this technique is that it is more secure and capacity is also high. The major drawback is that in some pixel no data will be embedded.

III. PROPOSED METHOD

So far we have observed from literature survey that each technique has some drawbacks. Most of the research work deals with low capacity. The improvement of capacity yields perceptible degradation of quality in the stego-image. Existing techniques are mainly based on the principle of embedding capacity and image quality. However, security is also a major concern of embedding secret information. In addition, very few among them are applicable for color images.

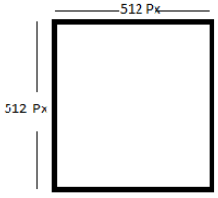
Hence, the immediate objective is to deal with the problems to be faced. First of all, this proposed method will work fine with color images with a control over quality degradation. All these will provide the best suitable environment for embedding secret bits.

There are two steps in our proposed steganographic technique.

I. Embedding
II. Extraction

Embedding

First of all, a 24 bit color image has been used as the cover image. The height and width of the cover image has been computed to obtain the total number of bytes in the cover image. For example, a 512 x 512 image ensured the total number of bytes as 512 x 512 x 3 = 786432.



Algorithm:

Step 1: Load the 24 bit color image as the cover image.

Step 2: Load the secret data to be embedded.

Step.3: The cover image is divided into 2 x 2 non-overlapping blocks.

Step 4: Read the Red/Green/Blue channel of the first 2 x 2 block.

Step 5: The six most significant bits of the first component

ISSN: 2278 – 7798 All Rights Reserved © 2016 IJSETR

are converted into decimal form and a modulo operation by 4 is performed with this value. The computed remainder value is used to decide the number of bits to be embedded. Then the quotient is again divided by 4 and the same process is followed until the quotient becomes zero.

Step 6: The two least significant bits of the first byte of the 2 x 2 block is used to decide the order of embedding. The secret data is embedded starting from least significant bit toward higher order bits position based on the indicator bits as follows:

Indicator bits	***Order of embedding***
00	Usual order
01	Complement
10	Reverse
11	Complemented reverse

Step 7: Repeat steps 4 to 6 for successive 2 x 2 blocks and excute the process till all bits of the secret data are embedded.

Step 8: Stop.

Extraction Algorithm:

Step 1: Load the 24 bit stego image.

Step 2: The stego image also is divided into 2*2 non overlapping block.

Step 3: Read the RED/GREEN/BLUE channel of the first 2*2 block rotationally.

Step 4: Last two bits of the First byte of the 2*2 block is checked to decide how the secret data was embedded.(i.e. if 00 then embedding is in usual order,.if 01 then embedding is in complemented order and so on as above table)

Step 5: First 6 bits are converted into decimal form and a modulo operation by 4 is performed with this value and the remainder value is used to decide howmany number of bits should be extracted. Then the quotient is again divided by 4 and the same process is followed until the quotient becomes zero. Then the required number of bits are extracted from the stego image and the secret data will be retrieved.

Step 6: Repeat steps 3 to 5 until all bits of the secret data are extracted from the stego image.

Step 7: Stop.

IV. CONCLUTION

Steganography can be used for hidden communication. Only 24-bit bitmap images are used in this proposed application. Other formats can also be used for making stego-images. The proposed technique is based on spatial domain which is simple and easy to understand. The degree of security, capacity and the image quality is tremendously enhanced as compared to existing techniques discussed in the literature. Since, the entire communication is made over an insecure channel, an intruder (others) can easily hack the stego-media for the motive of extraction of the hidden information. However, the proposed steganographic technique is designed in such manner that the hacker can't catch the hidden message as the sender and recipient both come to the agreement of confidentiality by keeping the embedding and extraction algorithms as private. Besides achieving the primary objective, the capacity of the proposed schemes is tremendously improved. The hash function used in the proposed scheme enhances the security of the embedded information. In addition, the quality of the stego-images is expected to be improved.

REFERENCES

[1] Pandey F., Gupta S. and Kumar S., " Information Hiding Using Image Steganography - A Survey", Journal of Basic and Applied Engineering Research, Print ISSN: 2350-0077, Online ISSN: 2350-0255, Volume 2, Number 10, pp. 854-859, April-June, 2015

[2] Al-Shatnawi, et al, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, , no. 79, pp- 3907 – 3915, 2012

[3] Bender W., Gruhl, N., Morimoto, and Lu A., "Techniques for data hiding", IBM Systems Journal, 35(3 & 4), 1996.

[4] Wu D. C., and Tsai W. H., "A steganographic method for images by pixel-value differencing" , Pattern Recognition Letters, 24(9-10), pp.1613–1626, 2003.

[5] Singh K. M., Singh L. S., Singh A. B., and Devi K. S., "Hiding secret message in edges of the image," Proceedings of International Conference on Information and Communication Technology, PP 238–241, 2007.

[6] Li X., Zeng T., and Yang B., "Detecting LSB matching by applying calibration technique for difference image," in Proc. 10th ACM Workshop on Multimedia and Security, Oxford, U.K, pp. 133–138, 2008.

[7] Ghosal S. K., "A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique", International Conference on Scientific Paradigm Shift in Information Technology & Management (SPSITM 2011) in collaboration with IEEE, Kolkata, 2011.

[8] Gutub A., "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol 2, No 1 (2010), 56-64, Feb 2010.

[9] Mondal J. K & Das D. "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012

[10] Tyagi V., et al, "Image Steganography using Least Significant Bit With Cryptography", Journal of Global Research in Computer Science (JGRCS), Vol 3, No3, March 2012

[11] Laskar S. A., et al, "High Capacity data hiding

ISSN: 2278 – 7798 All Rights Reserved © 2016 IJSETR

using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012

[12] Islam S, Modi M. R , et al, "Edge –based image steganography", *EURASIP Journal on Information Security* 2014, 2014:8

[13] Tseng H. W. & Leng H. S., "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Hindawi Publishing Corporation, Journal of Applied Mathematics, Volume 2013

[14] Bashardoost M., et al, "Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013

Soumen Bhowmik received his B. Tech (IT) degree from University of Kalyani and M. Tech (IT) from IIEST, Shibpur, West Bengal. He has published several research papers in different National and International Journals. His areas of interest are image steganography, real time video data processing, sensor network etc. He is the Life member of ISTE, IACSIT-Singapore, CSTA-ACM, ISOC- Switzerland etc.

Aditi Ghosh is pursuing M. Tech in the CSE branch under WBUT. She has completed her MCA. She has the interest in the field of image processing, image steganography, and network security.

Prof. (Dr.) Arup Kumar Bhaumik received his PhD (Engg) from IIEST, Shibpur. He was the former director of several RCCs and NITs. He has published several books, articles and research papers in national and international level. His areas of research are image big-data, advanced database, network of things, steganography, real time video data processing, sensor network etc. He is the life member of ISTE, IEEE, FOSET etc.

ISSN: 2278 – 7798 All Rights Reserved © 2016 IJSETR