LSB Embedding in Spatial Domain - A Review of Improved Techniques

Shaveta Chutani
Innocent Hearts Group of Institutions,
Jalandhar, India

Himani Goyal
Aryabhatta Group of Institutes,
Barnala, India

ABSTRACT

Steganography - the art and technique of hiding information in images, audio, video or text and other cover media has evolved and developed with time. Numerous improvements have been achieved with respect to security, robustness and capacity.

This paper presents a review of different LSB embedding techniques in Spatial Domain for image steganography. A variety of techniques which have evolved over time and have improved the basic LSB technique have been discussed. These techniques have also been compared on the basis of different parameters.

General Terms

Steganography, LSB.

Keywords

Steganography, LSB Embedding, Spatial Domain, Image, Review.

1. INTRODUCTION

Internet penetration has caused an explosive growth in the digital content exchange between various users. The legitimacy of the digital content is enforced using Digital Watermarking and Cryptography. Both of these techniques are different from Steganography, which attempts to hide some information in the digital content in such a way that the media carrying the secret message looks naïve. Steganography, in fact, attempts to hide some information in the digital content in such a manner that the presence of the secret information doesn't raise any eyebrows. Steganography is not a substitute of either Digital Watermarking or Cryptography; rather these are complimentary techniques which can ensure that the security of the information is achieved with greater success.

Steganography can be divided into different categories based upon the type of cover media chosen and the method of data embedding in it.

LSB Technique

The simplest form of Spatial Steganography is implemented by inserting the secret data into the Least Significant Bits. Different algorithms would insert the binary form of the secret data in 1, 2, 3 or 4-LSBs of the cover image. Though simplest to implement for RGB, Gray Scale or Binary Images and less susceptible to detection by Human Vision System (HVS), this approach makes the stego image more easily detected by various steganalysis techniques.

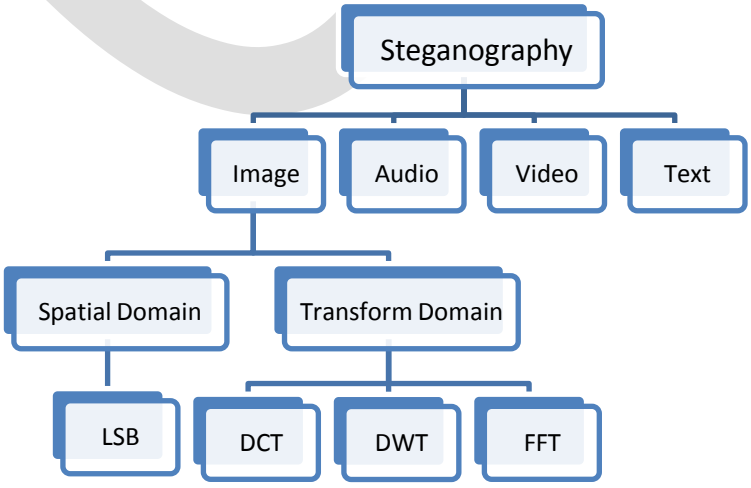

Figure 1: Various types of Steganography Techniques

LSB replacement steganography is a famous effective method which substitutes the least significant bits of the cover image for the secret bits [1]. For example,

The letter 'A' has an ASCII code of '65' (decimal), which is **01000001** in binary. It will require three consecutive pixels for a 24-bit image to store an 'A'.

Let's say that the pixels before the insertion are:

10000000, 10100100, 10110101, 10110101, 11110010, 10110110, 11100110, 10110011

Then their values after the insertion of an 'A' will be':

1000000**0**, 1010010**1**, 1011010**0**, 1011010**0**, 1111001**0**, 1011011**0**, 1110011**0**, 1011001**1**

Data hiding using LSB replacement is the simplest, convenient method which offers the advantage of being visually imperceptible to human eye and enhanced carrying capacity of the cover image.

However, presence of the secret message can easily be detected with the help of various statistical techniques like histogram analysis, χ^2 -attack, etc. There are also other numerous limitations posed by the LSB techniques such as non-robustness against compression, image editing and noise etc.

Different researchers proposed various ways to improve upon these constraints, the important ones being discussed below.

2. TECHNIQUES 'N' IMPROVEMENTS

2.1 BPCS

Rosanne English presented Bit Plane Complexity Steganography. BPCS technique [2] worked to improve the hiding capacity and effectiveness. The modus operandi of BPCS steganography is as follows:

The carrier image is divided into eight different bit planes which are further divided into small sized bit-plane blocks. According to the complexity, every block is categorized as noisy, artificially informative or naturally informative. Secret information is also divided into bit-plane blocks. This information replaces the original cover bit-plane block, if complexity of the cover bit-plane block is greater than threshold. However, if the complexity of the cover bit-plane block is less than threshold, a conjugation operation is performed to make it noisy and then block is ready to store secret information. Embedding is carried out starting from the lower bit-planes towards the higher ones.

Peipei Shi et al. [3] improved the concept of basic BPCS by introducing the concept of correlation between pixels. Pixels are highly correlated in higher bit-planes and less in lower ones. So, same embedding strength can't be set for all bit planes as it will have an adverse effect on histograms. Thus greater threshold is set for higher bit-planes while lower for lower bit-planes.

Therefore, Improved BPCS technique resists statistical attacks in a better way. It ensures good visual imperceptibility by embedding less secret information in higher bit-planes and more in lower bit-planes; consequently, ensuring greater data embedding capacity.

2.2 Multibase Notational Systems

Constantinos Patsakis et al. [4] proposed another approach in which pixel values can be decomposed in some other notational base rather than decimal or binary system. Zeckendorf [5] proved that every positive integer can be uniquely decomposed as a sum of non-consecutive Fibonacci numbers. Later on, [4] proposed a new method in which integer values of the colors were decomposed considering extended Zeckendorf's representation and generalized Fibonacci decomposition.

According to this method,

A sequence n_i of non-decreasing positive integers is complete iff

- $n_1 = 1$
- $n_1 + n2 + \ldots + n_k \geq n_{k+1} - 1, \forall k \geq 2$

Instead of altering the last bit of the binary representation of the color, any ordinal position of the Fibonacci representation of the pixel can be changed. The maximum value of the pixel i.e. 256 can be represented in 12 bits using extended Zeckendorf's form.

Now, the sender and the receiver sides have to agree upon the planes and the positions of the decompositions that are going to be altered.

This method makes the decomposition of a number more random. It is easier to embed information in gray scale images without leaving any noticeable traces, thus making it a very good alternative to LSB.

2.3 Pixel Value Differencing

Wu and Tsai [6] proposed a steganographic method based on PVD. They estimated the location of pixel by calculating the difference of two contiguous pixels. The number of embedded bits in these two pixels depends on the difference in their values. This concept was improved as PVDLSB by Wu and Wu [7] based on PVD and LSB techniques. When difference was small, they used LSB else they used PVD to hide.

Ki-Jong Kim et al. [8] put forward variable embedding length method to resolute the fall off boundary problem (FOBP) faced by the Wu and Tsai's PVD technique. This method uses the side information of the upper and left neighbouring pixels to calculate the new pixel value from the original one. The data is embedded in raster-scan order except for the pixels of first row and first column.

Later, Liaw, Wang and Chiu [9] proposed a new hiding method based on secret data division and PVDLSB. They divided the image into many non-overlapping pixel blocks. These blocks consisted of two contiguous pixels. Hiding capacity is dependent on the difference value of the two pixels in a block. The domain of the pixel values i.e., $[0, 2^a-1]$ is also divided into sub-ranges. The difference value of the pixels must lie in any of these sub-ranges. The number of secret bits to be embedded, n, is calculated using the formula $n = \log_2$ (sub-range). The n bit stream of the secret data is divided into two parts and inserted in pixel blocks based on modulus operation. At each step, care is

taken that after embedding, pixel values should remain within the domain of the pixel values. Moreover, the difference between the pixel values after embedding should remain in the same sub-range as before.

2.4 Modified Kekre Algorithm

MKA [10] is applied on 24-bit RGB color images. It uses 8-bit secret key to perform XOR operation to all bytes of the message. In MKA,

- Up to 5 LSB's of a pixel are used to embed the data.
- The number of LSBs to embed depends on the intensity pixel values as given in Table 1.

Table 1: Bit utilization in MKA Scheme

S. No.	Pixel Intensity	Data Bit to Embed	Matrix Entry	Utilize Bits
1	240-255	1	1	5
2	240-255	0	-	4
3	224-239	0	1	5
4	224-239	1	-	3
5	192-223	X	-	2
6	0-191	X	-	1

Later on, Mehdi Hussain et al. [11] improved the MKA algorithm with respect to two major aspects:

- Only lower intensity pixel has been used for data hiding.
- Maximum utilization of matrix which keeps the track of pixel where 5 LSBs are used for data embedding.

Table 2: Bit utilization in improved MKA

S. No.	Pixel Intensity	Data Bit to Embed	Matrix Entry	Utilize Bits
1	240-255	1	1	5
2	240-255	0	-	4
3	224-239	0	1	5
4	224-239	1	-	3
5	192-223	0	1	3
6	192-223	1	-	2
7	32-191	0	1	2
8	32-191	1	-	1
9	16-31	0	1	3
10	16-31	1	-	2
11	0-15	0	1	5
12	0-15	1	-	4

2.5 LSB Matching

The LSB matching [12] randomly adds or subtracts 1 from the value of the cover pixel if it doesn't match the secret message bit.

Later on, LSB Matching Revisited (LSBMR) [13] was proposed by Jarno, which allowed embedding of the same amount of information as LSB matching but with fewer changes to the cover image. Thus making the detection even harder than the previous one. Further, LSBMR has been improved upon by Quinhue Huang and Weimin Ouyang [14] by selecting suitable regions where LSB embedding is appropriate. Some areas in cover image such as smooth areas, frequent figure patterns and regions with regularly changed pixels are called fragile regions. A small change in such areas can have detectable changes on the image. So LSBMR method is not applied on such regions. This method successfully withstood HCF (Histogram Characteristic Function) steganalysis introduced by Harmsen et al. [15].

Ling Xi et al. [1] also improved LSB Matching algorithm based on modification of pixels with adjacent intensity as the modification of one pixel causes change in two adjacent bins of histograms which is undesirable. Thus there are high chances of being detected if histogram analysis is performed. Hence, to increase robustness, Ling Xi et al. [1] embedded two bits in a pair of complimentary pixels from the image with adjacent intensity by adding 1 to the pixel with lower intensity and subtracting 1 from the pixel with higher intensity. This is done so that after modification or insertion of secret bits, the histogram remains unchanged. To ensure the maximum number of complimentary pixels, the author has quite often chosen nature's images as cover images because such images ensure the continuity of intensity.

2.6 Compression Coding

Most of the techniques use a gray scale image or a color image as a cover image. However, few algorithms embed the secret image into the compression domain of the host image. Usually, only compression codes are transmitted via the internet rather than the image itself to save the transmission time or the bandwidth limitation. This can improve the efficiency for data transmission.

Using this concept, W. Du et al. [16] proposed an adaptive algorithm to embed data into VQ compressed images. This method adaptively varies the embedding process according to the amount of hidden data. The proposed method provides effective hiding and higher quality images.

Min-Hui Lin et al. [17] proposed A Novel Information Hiding Scheme Based on Block Truncation Coding (BTC).This technique embeds a binary image into the compression domain of a host image. The secret messages are sequentially embedded into the means of groups 1 and 2, generated during BTC and the bitmap of each block. Two substitution approaches were used in this method. The substitution for the means is based on simple LSB, and the substitution approach for the bitmap is based on minimum distortion algorithm.

Later Wu et al. [18] improved the Block Truncation Coding technique. The proposed method hides the secret data in

compressed images by modifying the bitmaps generated from BTC. The algorithm arithmetic is as under:

Divide the cover image and secret image into same sized blocks. Calculate the mean value of the pixels of each block. Compute the difference between the mean and all the pixel values of each block. Find the location of the pixel (p, q), whose difference from the mean is minimum. If secret bit is 1 and the number of 1's in the Bit Map is even or if the secret bit is 0 and the number of 1's in the Bit Map is odd, modify pixel (p, q) to 1 if it is 0, and otherwise modify it to 0. Based on the modified Bit Map, recalculate low mean X_L and high mean X_H.

2.7 Variable Length Embedding

Several techniques have been proposed through which the concept of variable length embedding has been applied to images for data hiding so as to ensure secrecy, security and robustness of hidden data.

Adnan Gutub et al. [19] proposed the pixel indicator technique which became the base for various variable length embedding techniques. This technique uses least two significant bits of one of the channels for existence of data in the other two channels. The indicator channels are chosen in sequence. The amount of hidden data is dependent on the least 2 significant bits of the indicator channel.

Mohammed Tanvir Farvez et al. [20] proposed RGB Intensity-Based Variable Bits Image Steganography. The technique uses one of the channels from red, green and blue as an indicator. The indicator sequence can be made random, based on a shared key between sender and receiver. Data is stored in one of the channels other than the indicator. The channel whose color value is lowest among the two channels, other than the indicator, will store the data in its least significant bits. Instead of storing a fixed no. of data-bits per channel, no. of bits will depend on the color value of the channel. The lower the value, the higher the data-bits to be stored.

Ahmed T. Al-Taani et al. [21] proposed a novel Steganographic method for gray Scale images for hiding information within the spatial domain. The proposed approach works by dividing the cover image into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel.

Later Kirti Upreti et al. [22] proposed a variable-length LSB based steganographic technique for data embedding in RGB image which was an improvement to all the previous algorithms. The secret message is converted into two kinds of plain texts by subsequent ASCII and binary conversions and suitable bit stuffing. Two cipher texts are obtained using RSA and IDEA algorithm. Both of these cipher texts are hidden in the cover image. One cipher text is used to determine the position for data hiding and the other cipher text is hidden in the LSBs of the color channel i.e. one which has minimum contribution in the image. Maximum intensity color channel is used to indicate which minimum intensity channel has how many bits of data embedded in it. Choosing such channels for hiding indicator and data bits, causes minimum distortion in the color of the pixels and such changes go undetected by human vision system.

3. CONCLUSION

This paper presents a review of the important techniques of LSB embedding in spatial domain. The techniques have seen a growth in the complexity of concepts developed and employed over a period of time but the basic requirements of imperceptibility in terms of invisibility, payload capacity and robustness against statistical attacks is of paramount importance. Though no single technique can be voted as the best, factors such as, size of the secret message, transmission channel capacity and availability of computing resources dictate the technique that can be used for determined purpose.

4. REFERENCES

[1] Ling Xi, Xijian Ping, Tao Zhang. Improved LSB Matching Steganography Resisting Histogram Attacks, IEEE 2010, pp.203

[2] Rosanne English. Comparison of High Capacity Steganography Techniques, IEEE 2010, pp.448

[3] Peipei Shi, Zhaohui Li, Tao Zhang. A Technique of Steganography Text Based on Chaos and BPCS, IEEE 2010, pp.232

[4] Constantinos Patsakis, Evangelos Fountas. Extending Fibonacci LSB Data Hiding Technique to more Integer Bases, in 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE 2010), pp.V4-18.

[5] Brown, J.L. Jr. "Zeckendorf's Theorem and Some Applications", Fib. Quart.2, 163-168, 1964

[6] D.C. Wu and W.H. Tsai. A Steganographic method for Images by Pixel Value Differencing, Pattern Recognition Letters, Vol. 24, Issue: 9-10, June 2003, pp.1613-1626.

[7] H.C. Wu, N.I. Wu, C.S. Hwang. Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Proceedings: Vision, Image and Signal Processing, Vol.152, Issue 5, Oct 2005, pp. 611-615.

[8] Ki-Jong Kim, Ki-Hyun Jung, Kee-Young Yoo. Image Steganographic Method with Variable Embedding Length, in International Symposium on Ubiquitous Multimedia Computing, 2008. pp. 210-213.

[9] Jiun-Jian Liaw, Wen-Sheng Wang, Min-Yen Chiu. A Data Hiding Method Using Secret Data Division and Pixel Value Differencing, in Fourth International Conference on Genetic and Evolutionary Computing, 2010. pp. 650-653.

[10] H.B. Kekre, Archana Athawale, Pallavi N. Halarnkar. Performance Evaluation of Pixel Value Differencing and Kekre's Modified Algorithm for Information Hiding in Images, International Conference on Advances in Computing, Communication and Control, 2009. pp. 342-346.

[11] Mehdi Hussain, Mureed Hussain. Pixel Intensity Based High Capacity Data Embedding Method, IEEE 2010.

[12] Toby Sharp, An implementation of Key based Digital Signal Steganography, in proceedings Information Hiding Workshop, Vol. 2137, Springer LNCS, 2001. pp.13-26.

[13] J. Mielikainen. LSB matching revisited, IEEE Signal Process. Lett., vol.13, no.5, pp.285-287, May, 2006.

[14] Quinhue Huang, Weimin Ouyang. Protect Fragile Regions in Steganography LSB Embedding, in 3rd International Symposium on Knowledge Acquisition and Modelling, 2010. pp.175-178.

[15] J. Harmsen and W. Pearlman. Steganalysis of Additive-Noise Modelable Information Hiding, in proceedings SPIE Security Watermarking Multimedia Contents, vol. 5020, 2003, pp.131-142.

[16] W. Du and W. Hsu. Adaptive Data Hiding Based on VQ Compressed Images, IEE proceedings Vision Image and Signal Processing, vol. 150, No.4, pp. 233-238, 2003.

[17] Min-Lui Lin and Chin-Chen Chang. A Novel Information Hiding Scheme Based on BTC, The 4th International Conference Computer and Information Technology, pp.66-71,2004.

[18] Xiaotian Wu, Wei Sun. Data Hiding in Block Truncation Coding, 2010 International Conference on Computational Intelligence and Security, IEEE 2010. pp.406-410.

[19] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen and Aleem Alvi. Pixel Indicator high Capacity Technique for RGB image based Steganography, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E. 18-20 March 2008.

[20] M.T. Parvez and A.A.A. Gutub. RGB Intensity Based Variable-Bits Image Steganography, IEEE Asia-Pacific Services Computing Conference, pp. 1322-1327, 2008.

[21] A.T. Al-Taani and A.M. Al-Issa. A Novel Steganographic Method for Gray-Level Images, International Journal of Computer, Information and Systems Science, and Engineering 3,1,2009.

[22] Kirti Upreti, Kriti Verma, and Anita Sahoo. Variable Bits Secure System for Color Images, 2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, pp. 105-107.