A Review of Digital Image Steganography using LSB and LSB Array

Mamta Jain  
Department of Computer Science and Engineering, Mody University of Science and Technology, Lakshmanagar, Rajasthan, India.

Saroj Kumar Lenka  
Department of Information Technology, Mody University of Science and Technology, Lakshmanagar, Rajasthan, India.

Abstract

Information exchange in the just about any cluster of computer has to be more secure in the era of cloud computing and big data. Steganography helps to prevent illegal attention through covering the secret message in a number of digitally electronically representative media, without hurting the accessibility of secret message. Image steganography methods are recently been helpful to send any secret message in the protected image carrier to prevent threats and attacks whereas it does not give any kind of opportunity to hackers to find out the secret concept. Inside a steganographic system secrets information is embedded inside of a cover file, to ensure that no one will suspect that anything perhaps there is inside carrier. The cover file could be image, audio or video. To really make it safer, the secrets information might be encrypted embedded then, it will be decrypted in the receiver. In this paper, we are reviewing some digital image steganographic techniques depending on LSB (least significant bit) & LSB array concept.

Keywords: LSB cipher, LSB array, steganography, cryptography, encryption, decryption, embedding.

Introduction

Since start of internet, the most important factors of information and communication technology has become the security of information, for that two techniques are employed cryptography and steganography. Steganography is a technique of secret communication by which one style of information is embedded into other information. The saying Steganography includes a Greek origin. This would mean covered writing. Numerous evident from the ancient history might be found as hiding messages within wax tablets and writing the content on messenger's body by Greece people. The most popular illustration of the steganography is, writing secret message on the paper with onion juice or ammonia salts along with the secret message might be then exposed by heating the paper. Once the cover object has material concealed in it, it is called stego-object. Various multimedia files may be used as carriers to cover the information. Typically steganography can be classified by carriers useful for concealing the data as image, video and audio steganography, where as in cryptography the secret data is encrypted with a key and sent on the channel. For such type of cases, intruders can observe that something is under communication, while he/she cannot steal the data unless the key is known. Whereas in steganography the person and/or

Steganography Classification

Following are the different classification of steganographic techniques, which is often employed for secure communication. Fig. 1 shows classification of steganography.

A. Categories of Steganography

Virtually all digital file formats works extremely well for steganography, but the formats which have been more suitable are those that has a high degree of redundancy. Redundancy can be defined as the bits of an object that offer accuracy far larger than necessary for the object’s use and display. An understandable method ended up being to hide a secret message in most nth letter of any word of any text. Text steganography using digital files just isn't used frequently since text files have a very tiny amount of redundant data. Digital images gives the large amount of redundant bits specific to digital representation associated with an image, images are classified as the most popular cover objects for steganography.

In audio carrier, similar techniques are used as image carriers. One unique technique to audio steganography is masking, which utilizes the properties of the human ear for hiding secret information imperceptibly.

The term steganography use the technique of embedding secret information within text messages and network control protocols utilized in network transmission. In the layers from the OSI network model, there exist covert channels where steganography can be utilized. A modified method for text steganography based on HTML tags and attributes is hypertext steganography. As HTML is abundant with tags and attributes, it will be easy to
communicate through online. By hiding the secret data in the source code of HTML, text steganography can be easily achieved [1].

![Figure 1: Classification of Steganography](image)

**Digital Image Steganography**

**A. Image Domain Steganography**

Image or spatial domain techniques embed secret information within the intensity value of the cover image pixels directly. Image domain techniques include bit-wise methods that use bit insertion and noise management and therefore sometimes characterized as “simple systems”. The image formats which might be the most appropriate for image domain steganography are lossless along with the techniques are typically relying on the picture format [1]. Fig. 2 shows the architecture of image steganography system.

**i. Least Significant Bit**

Least significant bit (LSB) insertion is the type of simple procedure for embedding information in a cover image. The lowest amount of significant bit (to put it differently, the 8th bit) of some or each of the bytes in an image is changed to amount of the secrets message. When using a 24-bit image, a certain amount of all of the red, green and blue color components can be used to store 3 bits in each pixel. Rolling around in its simplest form, LSB works by using BMP images, simply because they use lossless compression [1].

**B. Transform Domain Steganography**

Steganography from the transform domain requires the manipulation of algorithms and image transforms. These techniques obscure secret messages in most significant areas of the carrier image, which makes it better. Many transform domain techniques are in accumulation to the image format and the embedded secret information may continue with transform between lossy and lossless compression [1].

**i. JPEG**

The operation of embedding information during JPEG compression brings about a stego image that has an advanced level of invisibility, since embedding occurs from the transform domain. JPEG is the most popular image extendable on the web and the image sizes are small due to compression, thus making it the very least suspicious algorithm to use [1].

**C. Hybrid Domain Steganography**

**i. Patchwork**

It is a statistical technique which uses redundant pattern encoding to embed a message within the image. The algorithm adds redundancy on the hidden information, after which it scatters it through the image. Patchwork approach can be used independent of the host image and proves to be quite robust because hidden message may continue with transform between lossy and lossless compression [1].

**ii. Spread Spectrum**

In spread spectrum techniques, hidden details are spread throughout the cover-image turning it into harder to detect [1].

![Figure 2: Architecture of Image Steganography System](image)

**Literature Survey on LSB and LSB Array**

There are many of methods used to hide information in an image files. LSB and LSB array include the most common methods found in Image steganography. Here we are reviewing some methods according to LSB and LSB array techniques.

Chan and Chang [2] have used simple LSB technique with optimal pixel adjustment to improve the quality of stego-image. Zhang and Tang [3] suggested an improved LSB technique by selecting a set of cover image pixels at a time dynamically with the pseudo random number. They embedded n bits of secret data in every pixel of image using concept of addition and modular division operations. The n value is based on the length of embedded bit stream of secret data. In this technique, both security and capacity is targeted.

In other method, a new steganography methodology for secret data hiding is suggested. The binary representation of the hidden data is used to overwrite dynamically the LSB of each byte within the encrypted image. Security is increased by encrypted image and embedding [4].

Adaptive embedding technique is used to hide the variable number of bits in different image pixels. Using statistical analysis, find the embedding depth k in a image pixel to hide k number of bits by substituting k LSBs in that image pixel [5]. In this scheme, capacity and security has been enhanced.
Kekre et al. [6] suggested an image steganography LSB methodology for embedding variable number of secret data bits in different image pixels based on its value. They distributed the image pixel values into 4 different ranges, like R₁, R₂, R₃ and R₄. Now embedding of i bits in a image pixel in range Rᵢ for i=0, 1, 2, 3 is performed. The security of this algorithm is increased by using the adaptive bits. The capacity of algorithm is also enhanced by embedding up to 4 bits in some of the image pixels.

Mathkour et al. [7] used a spiral based LSB substitution technique to hide secret message in cover image. This technique is used RGB color channel component of cover image using LSB substitution. In this scheme divide the cover image into various parts and apply a different mechanism on each part of cover image. The methodology suggests three mechanisms corresponding to three sequences; start from corner, from centre and hybrid. They used two guidelines for the sequencing mechanisms; counter clock wise direction and clock wise direction. In this scheme only security is increased.

Mishra et al. [8] suggested a changed version of LSB technique. The secret binary data is divided into 8-bit blocks and the image is divided into 8-pixel blocks. A pseudo random number generator (PRNG) is used to embed the 8-bit message block into a selected 8-pixel image block. By using this message will be distributed over the entire image dynamically. Thus, by capturing LSBs and read by unknown party, no one can pass any secret information. If the integer value of each 8-bit message block is between 0 and 85, the embedding of these 8-bits takes place in the R plane of cover image. Similarly, values ranging from 86 to 170 are embedded in Green plane and values between 171 and 255 are embedded in Blue plane of cover image. In this mechanism only security has been enhanced. This method is better than simple LSB substitution, but the visual steganalysis observe that the distortion in the stego-image is remarkable by large amount of data embedding. The statistical analysis is done by plotting histograms. It is being observed that if the size of data changed in increasing manner then the variation in the histogram is mark able.

Swain and Lenka [9] proposed a double substitution cipher algorithm to encrypt the secret information. The encrypted information is then embedded to the cover image using the following scheme. In the first byte the 7th bit position is used for embedding, inside the second byte the 8th bit position is used for embedding, in the third byte the 7th bit position, in the fourth byte the 8th bit position etc. In this scheme, two levels of security is being provided.

Rosziati and Teoh Suk [10] suggested an image steganography algorithm using steganography imaging system (SIS). It is used to hide data inside the cover image. The receiver can use the same proposed system to retrieve the secret data back using a key. This secret key is calculated using the proposed scheme during the process of hiding the secret data. This algorithm maintains privacy, confidentiality and accuracy of the data by using secret key.

Swain and Lenka [11] suggested dynamic steganography, which is secret data bit dependent to insert one bit of data in 7th bit location of every pixel of image. In this technique capacity is only one bit per byte, but security is mark able.

A moderate bit substitution (MBS) data hiding methodology is given by Pharwaha [12]. In this technique, the pixel in the given cover image is skipped if all the first three positions of the LSB in it are one. The secret data bit is embedded at position next to first zero coming at any of the first three LSB positions in the image pixel. This process used random selection of bit position in an image pixel. A post pixel adjustment process is used to improve the perceptual quality of stego-image. In this scheme only security is enhanced.

Jain and Ahirwal suggested a novel adaptive embedding mechanism by using a private stego-key [13]. The private stego-key comprises of five dark level ranges that are chosen arbitrarily in the reach from 0 to 255. The chosen key demonstrates the five territories and every extent substitute’s diverse number of bits in LSBs. By utilizing this versatile implanting thought they can cover up to 4 bits in a few pixels, in this way it extraordinarily builds the limit notwithstanding security.

Swain and Lenka [14] proposed a procedure, in this a LSB steganography is utilized to insert two bits of message in two bit positions either (sixth and seventh), or (seventh and eighth), or (sixth and eighth) piece areas of a pixel relying upon the estimation of a index variable. The capacity is improved (2 bits per byte) and security is strengthened.

In a dynamic embedding based method, an evaluation function is used. Two LSBs are exploited. Some chose pixels are implanted. So limit is not enhanced, just security is improved [15].

In other method, element implanting in bit pattern of secret message is utilized. Three LSBs are abused in a pixel; however just two bits are inserted. Some chose pixels are implanted. So limit is not enhanced, just security is upgraded [16].

In another technique, element inserting taking into account bit pattern of secret message is utilized. Three LSBs are misused in a pixel; however just two bits are installed. Every one of the pixels is implanted. So limit is enhanced (2 bits for every byte) and security is upgraded [17].

Rig and Themrichon [18] presents a novel system for Image steganography in view of Huffman Encoding. Two 8 bit dim level picture of size M x N and P*Q are utilized as cover picture and secret picture individually. Huffman Encoding is performed over the secret picture/message before implanting and every piece of Huffman code of secret picture/message is inserted inside the cover picture by adjusting the least significant bit (LSB) of each of the pixel’s intensities of cover picture. The length of the bit stream of Huffman encoding and Huffman Table are likewise implanted inside the cover picture.

Manoj, Naveen and Anil [19] proposed a unique method for Image steganography depend on the data encryption standard (DES) utilizing the quality of S-Box mapping and Secret key. The preprocessing of secret image is conveyed by implanting function of the steganography methodology utilizing two novel S-boxes. The preprocessing gives higher state of security as extraction is unrealistic without the learning of mapping principles and secret key of the function.

Shamim and Kattamanchi [20] proposed a high limit information inserting methodology by the blend of
steganography and cryptography. In the process, a message is initially scrambled utilizing transposition cipher technique and afterward the encoded message is implanted inside a picture utilizing LSB insertion system.

Mamta and Parvinder [21] proposed a methodology used to insert content into dark picture (BMP). It empowers the client to furnish the framework with both content and cover, and get a subsequent picture that contains the concealed content inside. The framework utilizes the least significant bit (LSB) strategy to implant the secret content in picture after encode the secret content utilizing RC4 stream cipher system and store the content in non successive pixel in picture by utilizing variable hop value power of [22, 4, 8, 16, 32]. The Proposed framework intend to give enhanced dynamicity, security because of multi-level security construction modeling alongside faster installing and extraction prepare independent of size of inserted content.

Abdelmgeid and Hussien [22] proposed another technique that conceals the secret message inside the cover picture by representing to the secret message characters utilizing Braille system for perusing and composing for visually blind individuals. Braille framework utilizes six raised dots as a part of a deliberate course of action with two columns of three dots, known as a Braille cell, a 6-dot matrix which is the premise of Braille that can save more than one-fourth of the required space for embedding. Gutte, Chincholkar and Lahane [23] proposed a methodology in such way that, information is encrypted utilizing extended substitution algorithm and after that this cipher content is covered at a few LSB positions of the carrier picture. This calculation covers all sorts of digits, letter sets and math symbols. The encoded content is covered variably into the LSBs. In this way, it is a more grounded methodology.

In next method a strategy with four LSB arrays is proposed [26]. The four array, for example, LSB, LSB1, LSB2 and LSB3 are detailed independently by gathering the bits from the eighth (LSB), seventh, sixth and fifth position areas of the pixels individually. The cipher content is separated into four blocks. The first block is mapped and slided over the LSB array and inserted at most extreme matching part of the LSB array. Essentially the second, third and fourth blocks are embedded at most extreme portions of LSB1, LSB2 and LSB3 arrays individually. Both the security and limit has been made increased. The limit can be four times than that of [25].

### Table 1: Comparison between schemes proposed by different researchers based on LSB and LSB Array

<table>
<thead>
<tr>
<th>Researchers Articles</th>
<th>MSE</th>
<th>PSNR</th>
<th>Capacity</th>
<th>Visual Imperceptibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>H. B. Kekre, A. A. Athawale and P.N. Halarnkar [6]</td>
<td>0.14</td>
<td>56.42</td>
<td>Medium</td>
<td>Good</td>
</tr>
<tr>
<td>G. Swain and S. K. Lenka [17]</td>
<td>0.42</td>
<td>50.93</td>
<td>Medium</td>
<td>Better</td>
</tr>
<tr>
<td>S. A. Laskar and K. Hemachandran [20]</td>
<td>0.41</td>
<td>51.93</td>
<td>Medium</td>
<td>Better</td>
</tr>
<tr>
<td>M. Juneja and P. S. Sandhu [24]</td>
<td>0.35</td>
<td>49.35</td>
<td>Low</td>
<td>Average</td>
</tr>
<tr>
<td>G. Swain and S. K. Lenka [25]</td>
<td>0.52</td>
<td>69.12</td>
<td>High</td>
<td>Very Good</td>
</tr>
<tr>
<td>G. Swain and S. K. Lenka [26]</td>
<td>0.46</td>
<td>53.78</td>
<td>Medium</td>
<td>Better</td>
</tr>
</tbody>
</table>

### Conclusion

At the beginning with the paper, many experts have discussed on classification of steganography. Further it’s been classified in image steganography associated with image domain and transform domain. This paper covers and gives importance to the discussion on the major methods, techniques and algorithm of digital image steganography determined by LSB and LSB array which is used particularly in image domain. In the LSB techniques, substitution can be done up to 4 least significant bits. The color images can be embedded with direct LSB substitution. But if they are handled differently than the quality parameters can be improved. The LSB techniques give high capacity, but give moderate security as compared to techniques of other categories of digital image steganography. Steganography is the right approach for any secret communication in the internet. The comparison between schemes proposed by different researchers in the field of LSB and LSB array is shown in Table 1. This review paper will help researchers to recognize the idea and difference of LSB and LSB array methods in image steganography.
References


