Sobel edge detection technique implementation for image steganography analysis.

Smitha GL¹, Baburaj E²

¹Department of Computer Science and Engineering, Sathyabama University, Chennai, Tamil Nadu, India
²Department of Computer Science and Engineering, Narayananaguru College of Engineering, Manjalumoodu, Tamil Nadu, India

Abstract

Existing image steganographic methods lack in the complexity, which can be utilized by the radical to decode the images and neutralize the operations. Several methods have been proposed in order to combat this. Perhaps the most efficient method is Edge Adaptive based on Least-Significant-bit Matched Revisited (LSBMR) approach using Sobel edge detection. It is a famous type of steganographic methods in the spatial domain. In this paper we are proposing the latest Steganography algorithm-Edge Adaptive based on Least-Significant-bit Matched Revisited (EALSBMR) approach with the help of Sobel edge detection. The presented technique uses image-processing technique to detect edges and also comparison is developed based on MATLAB software. Sobel edge detection technique was applied on cover images to determine edges. Then sharper edges were exploited for embedding secret bits.

Keywords: Steganography, Pixel value difference (PVD), Methodology least significant bit (LSB) based steganography, Least significant bit matched revisited (LSBMR) algorithm, Edge adaptive least significant bit matched revisited (EALSBMR) algorithm, Edge adaptive based on LSBMR with the help of sobel operator.

Accepted on July 21, 2017

Introduction

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "writing" [1,2]. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography means that concealing one piece of knowledge at intervals another [3]. Image steganography is the subdivision of steganography where digital images are used as bearer file formats for information [4]. The merit of steganography with respect to cryptography is that the meant concealed data doesn’t engage observation to itself as an associate thing to search. Able to be perceived easily seen encoded information despite however indestructible bring to notice, and will in a group of people be inculpatory in the world wherever cryptography is prohibited. Hence, as well as cryptography is that the observe of protective the message contents only, steganography cares with hiding the fact that a concealed data is being transmitted , in addition as hiding the message contents [5,6]. The proposed technique uses image-processing technique to detect edges. Sobel edge detection technique was applied on cover images to determine edges. Then sharper edges were exploited for embedding secret bits [7].

Literature Review

The term Steganography as a result came in 1500s when the existence of Trithemius book on the world Steganographia [8].

Past

The term Steganography scientifically referred as covered or concealed writing. Its antiquated origins are half-tracked aback to 440 BC. Already the word Steganography was solely noticed at the tip of a period of fifteen hundred; the appliance of Steganography proceeds many kilo years. Ancient Chinese wrote messages on fine silk that was then fragmentize into a small ball and lined in wax. The courier then enveloped the ball of wax. Special “inks” were vital steganographic tools even throughout Second war. Throughout IInd world war, a method was introduced to reduce photographically a page of word into a dot but one metric linear unit in diameter, so conceal this photo in associate seemingly innocuous letter [9].

Present

The major these days steganographic systems utilizes transmission objects like image, audio, video etc. as cover media since individuals typically permits digital photos over
email and different net communication. Advanced Steganography utilizes the chance of concealing data as digital transmission files and additionally into the network packet level [10]. As an advanced way, by means of the cover medium, Steganography is classified as:

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography

Least Significant Bit Algorithm

In this section, the steganography algorithm of LSB is discussed. It is one of the ancient steganography algorithms that embed the message bits into the stego-image.

LSB description

It is a famous data-hiding technique used widely because of its straightforwardness. It passes the modified least significant bit of the stego-image pixels, which can change only the color tone [12]. This change is too small such that the human eye cannot notice it. The LSB hide out the message bits into the image pixels either in a sequential or randomized manner. It creates a path and replaces the least significant bits by the message bits. If the path is randomly formed then the pseudo random number generator PRNG is used [13]. The PRNG would be produced with some stego-key that is shared between the sender and receiver. In this way the message bits will be extended over the stego-image. LSBM provided distortion and resistance to the Steganalysis [14].

The LSB algorithm is represented in Figure 1. Initially a path is created that is used to select the pixels. These pixels are selected in an uncontinuous order based on a stego-key. For each bit of the secret message, a pixel is taken from the cover image based on the path. We would then change the least significant bit of the cover pixel by the bit of the secret message. The algorithm does not show the length of the secret message beside the message.

Example of LSB

Let’s assume that we want to fix the letter ‘A’ into a 24-bit cover image. The binary value of ‘A’ is 10000011. Let us assume that the three adjacent pixels of the image are the following:

(10110100 11010111 10011110)

(00011100 11110110 11010111)

(10001110 00011100 11100101)

The following pixels of stego-image are acquired after applying LSB steganography algorithm. Bits have changed because of the cover image pixels did not match the message bits.

(10110101 11010110 10001110)

(00011100 11110110 11010110)

(10001111 00011101 11100101)

The algorithm first selects a pixel \((x_i)\) consecutively. Then it checks whether the least significant bit of \((x_i)\) co-ordinate with the message bit \((m_i)\). Least significant bit of a pixel is the culinary bit which is the most right bit of a byte. If LSB \((x_i)=m_i\), then there should be no change otherwise LSB of \(x_i\) is substituted with \(m_i\). Then it selects the next pixel and message bit and checks whether they co-ordinate or not. This process continues till the end of secret message bits where all secret bits are fixed in the image.

Figure 2 shows two images of a gray-scale function. Figure 2a is the original cover image and Figure 2b is the stego-image with a message “Sathyabama University Ph.D Thesis Least Significant Bit Approach” is hidden inside it. The LSB algorithm is provided and the stego-image Figure 2b is formed. The pixels are selected uncontinuously using PRNG.

Analysis of LSB

The LSB steganography algorithm is easy to comprehend. Furthermore, appliance of the LSB algorithm includes low CPU cost and complexity. This section presents some features the algorithm conserve.
Invisibility: The LSB algorithm utilizes the fact that human eyes do not recognize the small color modifications. Karaman et al. [15] stated that modifying up to 4th least significant bits are not recognizable by human naked eye. For that reason many algorithms are suggested as improvement to this simple LSB-approach to conceal the secret message in different level of least significant bit [13].

Capacity: The concealing capacity rate of the algorithm for an 8-bit depth gray-scale image is at minimum 1 bpp and for a 24-bit image is minimum 3 bpp. “bpp” is a measure used to find the capacity rate of implementing the message bits into a pixel and stands for bit per pixel. In other words, bpp stands for number of secret bits in which a pixel of a cover image can hold. It can be noted that as the stego-image size increases, the capacity of implanting the secret message increases. This indicates that a significant amount of information can be concealed using the LSB algorithm. The maximum implanting rate of 1 bpp means the likelihood of the expected variety of bits modifications is 0.5.

Security: The stego-key is shared between the sender and receiver to satisfy the correct removal of the secret message bits. The stego-key makes sure that the security is preserved and only the sender and receiver who possess the key can remove the secret message.

**Limitation of LSB**

The LSB algorithm is commonly used as a simple image steganography technique. However, this algorithm has many disadvantages related to undetectability and robustness features.

Undetectability: It is one of the most important features in steganography. The bigger the alteration is applied to the stego-image, the extra noticeable elements will be introduced. If the payload capacity of the LSB algorithm is greater, the statistical properties of the stego-image varies with the cover image. Randomness occurs when the least significant bits are modified in the cover object. This randomness can be found out by some statistical analysis techniques [15].

Some stego-images can be beaten with visual analysis of the LSB of stego-image. This is called a visual attack. The idea of visual attacks is to disjoin some parts of the stego-image and present them in a way which helps a person trying to search for noise [16]. Figure 3a displays a cover image and Figure 3b Image plane with the help of least significant bits. The white is displayed when the pixel’s least significant bit=1 and black when least significant bit=0. From Figure 3b you can see the least significant bits which are not random and represent the content of the cover image. Thus, alteration of these bits in number of parts of the image will abandon visual abnormalities or noises. For example changing the bits of the plate of the first object on the right (black part) will insert some noises and antique. This leads to the detection of the secret information by simply determining the LSB plane of the image.

The process of determining and using the histogram of the image to detect the existence of hidden information is called histogram attack. Histogram attack is a statistical approach for steganalysis applied on LSB approach [17]. One of the most well-known steganalysis techniques is the RS-analysis. RS analysis is a steganalysis method for finding the stego-images that are based on LSB. It is used to estimate the size of the concealed data. RS makes changes to the least significant bit plane. Then the altered bits with some differentiation function which are used to classify some sets of pixels. Those sets are counted and some calculations are done to estimate the message size [18]. It determines the lack of equality imbalance established to the picture when many LSBs changes. Asymmetry artifacts occur because at the implanting process the even values are always increased while the odd values are always decreased. This occurs when the secret bit does not co-ordinate the pixels bit. This effect is introduced into the histogram and makes the concealed information detectable.

**Figure 3. (a) Cover image (b) LSB plane of the cover image.**

Robustness: LSB is unsafe to image processing such as cropping, resizing, scaling, rotating and lossy compression which will destroy the hidden message. For instance, a stego-image is changed to another file format; the resulted format uses lossy compression. In that case the concealed information is destroyed and cannot be rebuilded. All the approaches based on LSB are not robust against some image processing. As mentioned earlier robustness is not a crucial feature of steganography.

**Improvement of LSB**

Another method which is proposed to modify the invisibility of the stego-image quality is the LSB matching (LSBM) algorithm. This method donot replace the least significant bits in the stego-image as like the above method. +1 or -1 (± 1
Subsequently Mielikainen [20] suggested LSB matching revisited algorithm (LSBMR). To solve that limitation in LSB change of a pixel with its adjacent pixels [20]. Sobel detection the secret bit, the algorithm randomly adds 1 and it becomes 64 change is very notable. As the change gets lesser, the edges become honorable. Small changes to the pointed edges will be neglected. The target of this method is to maintain the statistical and visual features of the cover image and to raise security respectively. The compression and encryption will only be utilized for implementing an application. In the experimental method and result this step is neglected.

Using compression will reduce a number secret bit which leads to decrease number of modified pixels. The compression method utilized is deflating. Deflate is one of most usual compression methods, operators are utilized where Sobel operator is a mutually perpendicular gradient vector field operator. Gradient is an assessing of texture information given on these edges. A Sobel edge detection method has a merit of low computational time. Hence employing it in steganography doesn’t add any huge complexity.

Sobel Operator Based Edge Adaptive Image Steganography based on LSBMR

One major elemental feature of an image are edges. The main data of the image has been carried out by edges. Edges are named as the brightness change of pixels value in a block of local pixels. The sharp edges are named as the edges where the change is very notable. As the change gets lesser, the edges become honorable. Small changes to the pointed edges will be minimum visible to human eyes since the complication of texture information given on these edges. A Sobel edge detection method has a merit of low computational time. Hence employing it in steganography doesn’t add any huge complexity.

The presented method utilizing Sobel method utilizes Sobel’s edge detection method in order to obtain edges. After that these edges are handled for combining work. For lesser combing rates the pointed edges are utilized for belonged data. When the rates rise, the method invariably is regulated to utilize small pointed edges. As the range is attained highest, then all the flat edges are delivered to be utilized. The target of this method is to maintain the statistical and visual features of the cover image. Based on the secret data and the gradient of the cover image content for data hiding units can be selected. In this section, firstly main points of sobel edge detection technique will be discussed. After that detail explanation of the presented method will be described.

**Overview of sobel edge detection**

The proposed embedding method utilizes Sobel edge detector on every 3 × 3 non-overlapping block of the cover image. To conduct detection in edge detection methods, operators are utilized where Sobel operator is a mutually perpendicular gradient vector field operator. Gradient is an assessing of change of a pixel with its adjacent pixels [20]. Sobel detection is a gray weighted technique of the next to points in 2 directions. It founds edges of the point depending on its next to points. Gradient of point $v(i,j)$ of a position $ij$ consist of two first derivatives in i-direction and j-direction such that it utilizes $3 \times 3$ neighboring of the point:

$$G_i = \{v(i + 1, j - 1) + 2v(i + 1, j) + v(i + 1, j + 1)\}$$

$$G_i = \{-v(i - 1, j - 1) + 2v(i - 1, j) + v(i - 1, j + 1)\}$$

$$G_j = \{f(i - 1, j + 1) + 2v(i, j + 1) + v(i + 1, j + 1)\}$$

$$G_j = \{-v(i - 1, j - 1) + 2v(i, j - 1) + v(i + 1, j - 1)\}$$

The gradient vector field is determined for each point $v(i,j)$ is given below:

Gradient vector field $(i, j) = |G_i| + |G_j| \rightarrow (2)$

$$
\begin{bmatrix}
-1 & 0 & 1 \\
-2 & 0 & 2 \\
-1 & 1 & 2 \\
\end{bmatrix}
\rightarrow (3)
$$

Figure 4 explains the algorithm of Sobel edge detection algorithm. This algorithm is given to edge detection to be used with our proposed technique. Next portion explains about the hiding of data and process of extraction of the presented method.

**Data hiding process**

Step-1. At First the text is compressed and concealed using stego-key1. Compression and encryption are utilized to decrease the amount of data needed to be concealed in a cover image and to raise security respectively. The compression and encryption will only be utilized for implementing an application. In the experimental method and result this step is neglected.

Step-2. Compression will reduce a number secret bit which leads to decrease number of modified pixels. The compression method utilized is deflating. Deflate is one of most usual method adopting lossless compression algorithm [21]. Numerous implementations utilize this method as it has a high completion [22]. Deflate utilizes combination of LZ77 and Huffman coding [21]. The LZ77 method uses the notable word as an entry in the dictionary. If a duplicate string is seen, then the second string is restored by an index of dictionary of the duplicate string [21,22]. The Huffman coding is a statistical probability for estimating the occurrence of all symbols. Then a Binary Tree is established according to probability size from downward to upward and encoding is conducted [21].

Afterward, AES encryption method is utilized to encrypt the compressed text. AES (Advanced Encryption Standard) is one of most general encryption algorithm utilizing Symmetric Encryption algorithms [23]. As mentioned earlier, in symmetric encryption algorithm the same key is utilized for encryption and decryption. The AES algorithm is a block cipher with a key having size of 128, 192 and 256 bits. AES 128-bit data block-cipher works on 4 × 4 byte matrix [24]. Numbers of transformations are given to convert the plain text to cipher text. Four transformations are implemented; Sub
Bytes restores one byte with another. Shift Rows shifts the rows cyclically with a predetermined offset. Mix Columns is linear transformation that embeds 4 bytes of each column. Key Addition gives bitwise XOR of the data block with round key [24]. Encryption is utilized with the proposed steganography algorithm to add another level of security. The key given for encryption at the sender side is same as the key utilized at the receiver which serves as stego-key1 [25].

Step-2. The image is split up into 3 × 3 non-overlaying set. We determine the gradient values on the basis of Figure 4. One of each middle point of the 3 × 3 block of picture elements. The edge detection is not given on all pixels because any modification on one point will change all the pixels around it. The readjustment is then very complicate in terms of application and time complexity. After calculating the edges values the cover picture is transformed to bitmap vector V consisting of all the picture elements. The gradient vector field of all points in sequence is then stored in a vector Gr.

Figure 5a points out the cover gray-scale image of Shreya of size 512 × 512. Figure 5b points out the detected edges of the image Lena.

Step-3. The gradient intensity is calculated on the basis of the secret data M size and the picture content. The greater the gradient vector field is, the keener the edge is.

Let the set R consists of all the picture elements xi that is on edge having their gradient vector field (Gr(xi)) higher than or equal to intensity g. Then R is a set that is defined as:

\[ R(g) = \{ x_i | Gr(x_i) \geq G, i = 0, 1, 2, ..., n - 1, \forall x_i \in V \} \rightarrow (4) \]

Where n is the picture size and intensity G is found by

\[ G = \max_g \{|R(g)| \geq |M|\} \rightarrow (5) \]

\[ g \in \{0, 10, 20, ..., 370, 380, 390, 400\} \]

and \(|R(g)|\) is the numerals of the element in the set R(g) and \(|M|\) is the secret message size. After tested some empirical experiment g=400 is found to be the best to begin with. Every time decrease of g with 10 if it is not sufficient for keeping all the information. Till zero is arrived that means level areas alongside the pointed one is utilized for embedding the information.

Step-4. After determining the set consisting of satisfactory picture elements, since LSBMR needs a unit of two picture elements after that they are taken from the set R(g) based on PRNG using stego-key2. The first pixel will hold mi and correlation between two pixels will hold mi+1 based on (3).

The image Lena in Figure 5a is taken as cover image to embed secret information of 856 bits. Figure 6 points out the part of the resulted image such that black dots explain the locations of the pixels utilized for embedding the secret message’s bits. The calculated gradient is G=230. The final image (Figure 6) confirms that only sharp edges are utilized for data embedding.

Step-5. The side data G is embedded in the picture in an adjusted place familiar to the transmitter and receiver. Hence the gradient vector fields of the final image’s edge are determined once more. The recent gradient vector fields are contrasted to the image gradient of the cover to guarantee that the adjusted picture elements gradients are once again above or equal to the intensity G. Otherwise re-adapt and after that sum ± 2 selectively to the pixel of the neighbor. Then again determine the gradient if yet not in the extend, after that sum another ± 2. Do again the re-adaptation until the right one is obtained. Numbers that reduce below zero or above 255 are re-adapted on the basis of the formula (6) and T=0. The stego-image is then obtained.

\[ (y'_1, y'_2) = \text{argmin}(e_1, e_2) \{(e_1 - x_i) + |e_2 - x_i + 1|e_1, = y_i + 4k_1, e_2 = y_i + 1 + 2k_2, |e_1 - e_2| \geq T, 0 \leq e_1 \rightarrow (6) \]

\[ e_2 \leq 255, 0 \leq T \leq 31, (k_1, k_2) \in Z \}

The algorithm of the proposed method is given in Figure 7. Figure 7a explains proposed schema of the data hiding and Figure 7b explains data extraction process.
In general, the proposed algorithm utilizes region adaptive scheme to the spatial LSB domain. The Sobel edge detection method is utilized as the criterion for region identification. LSBMR is used as the data-hiding method. The proposed schema applied on the Lena image with hiding 1000 bytes of information. Figure 8 represents the stego-image.

**Table 1. Comparison of different algorithms.**

<table>
<thead>
<tr>
<th>Type of Algorithm</th>
<th>SNR</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>EALSBMR with SOBEL Operator</td>
<td>39.6322</td>
<td>43.6168</td>
</tr>
<tr>
<td>Simple LSB</td>
<td>16.4989</td>
<td>22.0814</td>
</tr>
</tbody>
</table>

**Conclusion**

We have surveyed the two algorithms that are generally used for image steganography. The application realizes that a stego image where the personal data is embedded and is safeguarded with a password which is highly secured. The main intention of the paper is to obtain a steganographic application that yields good security. We are presenting the Edge Adaptive based on Least Significant Bit Matching Revisited (EALSBMR) algorithm with the help of Sobel operator in this paper for obtaining the application which is faster and reliable and compression ratio is moderate compared to EALSBMR algorithm. The presented technique utilizes image-processing technique to detect edges whose comparison is given in Table 1. Sobel edge detection technique was given on cover images to obtain edges. Then keener edges were exploited for embedding secret bits. The proposed technique provides a good balance between the security and the image quality. Simulation results in MATLAB provide the effectiveness of the proposed method. The sobel edge detector helps the new scheme in generating a better quality stego image. The proposed sobel edge detector approach results improvement in the quality of an image as compared to simple LSB based technique.

The proposed EALSBMR with SOBEL Operator approach can be implemented in the future for following real world applications:

1. The proposed approach can be implemented to other cover medium such as audio/video.
2. The proposed approach can be applied on gray scale images.
3. The proposed approach can be used for frequency domain, type of data embedding.
4. The proposed approach can be implemented for real time Image Authentication System.

References
6. Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong 2002.
12. Mare SF, Vladutiu M, Prodan L. Decreasing change impact using smart LSB Pixel mapping and data rearrangement. 11th International Conference on Computer and Information Technology 2011.

*Correspondence to
Smitha GL
Department of Computer Science and Engineering
Sathyabama University
India