ADAPTIVE IMAGE STEGANOGRAPHY USING PIXEL INTENSITY DIFFERENCE

Kunal Ashok Shinde,
Omkar Rajendra Gandhi,
Somanath Rohidas Langute
Dept of CSE,
Nagaraj V. Dharwadkar
HOD of CSE dept Rajarambapu Institute of Technology, Rajaramnager

Abstract—In this digital world the Internet has become so popular and billions of people are using it. On various platform, web applications as well as standalone applications there is a need of Internet. For this purpose various techniques like cryptography, data encryption/decryption, and data hiding algorithms are invented. But use of these techniques was not too secure and hackers easily stole the secret message. To ensure high security of confidential data a new technique was invented known as “Steganography”. In this paper we a new a new steganography scheme which is very efficient with respect to data hiding capacity and distortion. The main approach for this algorithm is based on pixel intensity difference.

Index Terms—Cryptography, Steganography, Intensity, hacker

I. INTRODUCTION

Steganography is the process hiding the data into another data that cannot be detected easily through the open eyes. Image Steganography is the part of Steganography in which images are used for hiding the secret data. The Word came from Greek words “stegos”. which means “cover” & “grafia” which means “writing” so “Covered Writing” is the meaning of Steganography Though Steganography sense like Cryptography but there is some differences between them which split these two terms Cryptography always concern about keeping the content message secret but Steganography is concern about keeping the message secret.

The terms which are important in Image Steganography are Image Quality after embedding the secret data and ability of the image to keep maximum confidential data as possible. There are so many algorithms and methods available for Image Steganography which gives the best implementation of Image Steganography. These algorithms have very well embedding capacity with minimum distortion compare to original image.

II. HISTORY AND BACKGROUND LITERATURE SURVEY

a) V.Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz have proposed [1] experimental work done Color Image Steganography based on Pixel Value Modification Method Using Modulus Function. In this proposed system introduce approach known as Pixel Value Modification (PVM) using modulus function.

Proposed method cover image divided into three color planes (Red, Green, Blue), this scheme use modulus by 3 function. After dividing pixel value we get separate M*N matrix. And pixel embedded into cover image by sequentially manner suppose

1. 1st red secret pixel embeds into 1st pixel in red of cover image.
2. 1st green secret pixel embeds into 1st pixel in green of cover image.
3. 1st blue secret pixel embeds into 1st pixel in blue of cover image.

Limitation:

1. It only suitable for 24-bit pixel image. Not on gray scale image, because less cover image embedding capacity.
2. It includes high calculation overhead.

b) Weiqi Luo, Fangjun Huang, Jiwu Huang have proposed [2] experimental work done Edge Adaptive Steganography Based on LSB Matching.

Proposed Scheme:

To overcome the limitations of the “Least Significant Bit” Method the new technic for hiding the secret message was proposed known as “Least Significant Bit Matching Revisited”. The paper extends the LSB Matching Revisited Scheme and proposes a new idea. According to the edge adaptive scheme the selection of the region for hiding secret data is based on following two factors:

1. The size of confidential data.
2. The difference between two successive pixels of the cover image.

Based on the smoother area and edges of the cover image, the sharper edge region is used to hide secret data, when embedding capacity of message is low. When the embedding capacity is get increased then additional region is selected for hiding secret data by adjusting some boundary conditions. According to the pseudorandom number generator some minor changes are done in the LSBMR method, if secret bit is not similar as LSB of the main image then one bit is increased or decreased randomly with respect to pixel value. The normal LSBMR approach deal with a single pixel or pair of pixel without examining the difference between pixels or neighbor pixels.

K.E. Society's

RAJARAMBAPU INSTITUTE OF TECHNOLOGY
Limitation:

1. In the LSB method it is very easy to detect if we try to manipulate the stego-image. The stegoimage will get destroyed if we perform certain operations like compression, scaling, rotation etc.
2. The secret message size is depends on the size of the image this means the message size have to keep smaller than the original image.
3. Low secure and easily identified by the attacker.
4. Message hiding capacity is low.
5. Less secure and poor quality of stego-image with respect to smoother region of an image.

III. HELPFUL HINTS

A. References

B. Abbreviations and Acronyms
LSB: Least Significant Bit.
TPVM: Tri-Pixel Value Modification
APVM: Adaptive Pixel Value Modification
PVD: Pixel Value Difference
EMD: Exploiting Modification Direction.
LSBM: Least Significant Ration Matching Revisited.
MSE: Mean Square Error.
PSNR: Peak Signal to Noise Ratio.

C. Equations

\[
MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (I(i,j) - K(i,j))^2
\]

Where,
- \(m \times n\) = Total no of pixels.
- \(I(i, j)\) = Prediction values of new image.
- \(K(i, j)\) = True values of original image.

\[
PSNR = 10 \cdot \log_{10} \left( \frac{MAX^2}{MSE} \right)
\]

\[
= 20 \cdot \log_{10} \left( \frac{MAX}{\sqrt{MSE}} \right)
\]

\[
= 20 \cdot \log_{10} (MAX) - 10 \cdot \log_{10} (MSE)
\]

Where,
- PSNR = Peak Signal to Noise Ratio
- Max = Maximum intensity values = 255
- MSE = Mean Square Error

IV. PROBLEM DEFINATION

i. PROBLEM DESCRIPTION

The literature survey on the studied schemes has some limitations with respect to some factors. These factors are manipulation of image, embedding capacity, distortion, calculations. So we proposed a new method to overcome these limitations known as “Adaptive Image Steganography using Pixel Intensity Difference”.

ii. PROPOSED SYSTEM AND METHODOLOGY

i. ALGORITHM

1. Select cover image.
2. Scan cover image row by row (Raster scan). Convert cover image into binary format stored into buffer, and calculate pixel intensity difference pixel by pixel.
3. Convert secret data into binary format.
4. If pixel intensity difference is same, no embed secret data into cover image.
5. If pixel intensity difference is different then select low intensity pixel and embed data at LSB-bit, LSB-1 bit. And select contiguous higher intensity pixel embeds data only at LSB bit.
6. If pixel intensity difference is then repeat step 5 until secret data not completely embed.

ii. FLOWCHART

Start
Select Cover Image
Scan Whole image using Raster scan (row)
Calculate pixel intensity difference through pixel by pixel
If all pixel intensity is same True
If all pixel intensity difference is same then no change (All pixel intensity is same)
Select the low intensity pixel one by one based on pixel intensity difference. And place data at LSB.
Next which pixel has high intensity place data bit only at LSB bit through one by one
Stegoimage
Final Output image
End
V. RESULT AND DISCUSSION

The above image is a color image in which every pixel represents 24 bits that is:
- Red: 8 bit
- Green: 8 bit
- Blue: 8 bit

Binary representation of pixels is as follows:
- Pixel A: Ar = 125 = 01111101
- Pixel B: Br = 99 = 01100011
- Pixel C: Cr = 127 = 01111111
- Pixel D: Dr = 99 = 01100011

We have to hide secret data “Hi”

Now the conversion of Hi into binary data is:
H = 72 = 01001000
i = 105 = 01101001

According to our proposed algorithm suppose the pixel B having low intensity than pixel A.
So that we are going to embed two bits of secret data at LSB & LSB-1 position in Pixel B. Whether pixel A having high intensity than B we will embed only one bit secret data at LSB position.

Change in bits: Bold
No change: Bold with Underline

Pixel B:
- Br = 99 = 01100011
- Ar = 124 = 01111100
- Bg = 98 = 01100010
- Ag = 197 = 11000100
- Bb = 101 = 01100101
- Ab = 126 = 01111110

Pixel D:
- Dg = 101 = 01100101
- Cr = 127 = 01111111
- Db = 95 = 01011111
- Db = 104 = 01101000
- Cb = 95 = 01011111

Original Pixel Values of color Image

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>125</td>
<td>97</td>
<td>127</td>
<td>99</td>
<td>98</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>197</td>
<td>100</td>
<td>95</td>
<td>105</td>
<td>120</td>
<td>127</td>
<td></td>
</tr>
</tbody>
</table>

Change pixel value in cover image

<table>
<thead>
<tr>
<th></th>
<th>124</th>
<th>99</th>
<th>127</th>
<th>99</th>
<th>96</th>
<th>126</th>
</tr>
</thead>
<tbody>
<tr>
<td>196</td>
<td>98</td>
<td>127</td>
<td>101</td>
<td>105</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>101</td>
<td>95</td>
<td>104</td>
<td>120</td>
<td>120</td>
<td></td>
</tr>
</tbody>
</table>

MSE = \( \frac{1}{m*n} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i,j) - K(i,j)]^2 \)

PSNR = \( 10 \cdot \log_{10} \left( \frac{\text{Max}}{\text{MSE}} \right) \)

\( \text{MSE} = 3 \) db

\( \text{PSNR} = 43.3596 \) db
I. FUTURE WORK

The algorithm can be made more secure by changing the encryption technique of data. We can also add new cryptographic algorithm to improve the confidentiality.

II. CONCLUSION

We have designed a new method which overcomes the limitations of the existing schemes. The proposed scheme on color image steganography provides more embedding capacity as well as less distortion of the image.

REFERENCES


