A Secure and Efficient Spatial Domain Data Hiding Technique based on Pixel Adjustment

Shabir A. Parah\textsuperscript{1}, Javaid A. Sheikh\textsuperscript{2}, G. M. Bhat\textsuperscript{3}

\textsuperscript{1,2}P.G. Department of Electronics University of Kashmir, Hazratbal, Srinagar, J and K, India-19006.
\textsuperscript{1}shabireltr@gmail.com  \textsuperscript{2}sjavaid_29ku@yahoo.co.in

\textsuperscript{3}University Science Instrumentation Centre (USIC) University of Kashmir, Hazratbal, Srinagar, J and K, India-190006.
\textsuperscript{3}gmbhat_ku@yahoo.co.in

Abstract. A spatial domain hiding technique based on Intermediate Significant Bit (ISB) embedding and pixel adjustment has been investigated and presented in this paper. The data has been embedded in the cover image at the locations pointed to by Pseudorandom Address Vector (PAV). The image quality deterioration of the stego-image has been taken care of using pixel adjustment technique. The pseudorandom embedding of data enhances the security of the hiding scheme. The comparison of our method with an existing technique shows that proposed technique is capable of providing better quality stego-images even if the payload is slightly more. A 3dB increase in PSNR in case of proposed technique substantiates the argument.

Keywords: Encryption, Embedding, Information security, Pseudorandom.

Introduction

In the contemporary digital age information assumes a great importance, especially if the information is of classified nature; pertaining to national security, military operations, bank transactions and trade secrets. To prevent misuse of critical information by unauthorized people, the information security systems have to be implemented. Data encryption (Cryptography) \cite{1, 2}, conventionally, has been used as a security tool to safe guard sensitive data against passive attacks like eavesdropping. Cryptography scrambles a message and converts it in a disguised form using a secret key so that so it cannot be understood by the adversary. Although cryptography enhances the security of the secure data being transmitted, but the masquerading form of the encrypted message directly arouses suspicion from an adversary and it increases chances of malicious attack on the encrypted message \cite{3}.

Steganography of late flourished as another potent tool for secure communication \cite{4, 5, 6}. In steganography, the secret message is embedded into a cover medium (Image, Video, Text), and then sent to the receiver, where extraction of the secret message from the cover message takes place. After embedding the secret message, the cover image is called a stego-image \cite{7}. This image should not be distinguishable from the cover image, in order to avoid any prima-facie
presence of embedded message. Steganography actually belongs to a broader field of data hiding [8] which also encompasses digital image watermarking [9, 10].

Least Significant Bit (LSB) substitution is one of the earliest and computationally efficient hiding methods [11]. This scheme however, suffers from a serious drawback viz. the embedded data is easily lost when various image processing operations are applied to the stego-image. Further, for storing stego-image (grayscale) in memory or to reduce transmission time, certain applications discard LSB of image reducing it to a seven bit image instead of eight, which is again a serious challenge for LSB embedding. These problems can be addressed by embedding data in Intermediate Significant Bit (ISB) planes. An ISB based data hiding technique has been reported in [12], but this technique suffers from a disadvantage that data is embedded in the ISB plane in sequential order, making it easy for an adversary to extract the data.

A data hiding technique which embeds encrypted secret data in 3rd ISB plane of the cover image is presented in this paper. The embedding locations are determined by contents of PAV. For enhancing perceptual transparency of the stego-image embedding is followed by Pixel Adjustment.

**Proposed spatial domain data hiding system**

A block diagram of the proposed spatial domain data hiding system is shown in Fig.1.

![Fig. 1 Proposed data embedding system](image)

The system employs Intermediate Significant Bit (ISB) plane data hiding at the locations determined by PAV [13]. This is followed by Pixel adjustment algorithm. The data to be hidden in the cover image is first encrypted in the scrambler using a private key K1. The encrypted data has been embedded in the 3rd ISB plane of the cover image. The locations are determined by PAV, generated using a private key K2.

The proposed data hiding system uses 256 × 256 size test images as cover medium. Thus,
the number of pixels, in each cover image is 65536. The number of addresses in PAV for such a system is 65536. For such an address generator 16 bit key K2 has been used.

**Data hiding and need for Pixel Adjustment**

The main problem of LSB substitution technique viz. LSB removal (used for improving transmission rates, and reducing the memory sizes to save the stego-image) can be addressed by embedding data in the higher order bit planes. This however deteriorates stego-image quality, as explained as follows. The Peak Signal to Noise Ratio (PSNR) of a stego-image when compared with its cover image is given by Eqn. 1:

\[
PSNR = 10 \times \log_{10} \frac{255^2}{MSE}
\]  

(1)

\[
MSE = \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} (x_{j,k} - x'_{j,k})^2
\]  

(2)

Where \(MSE\) represents Mean Square Error and is calculated between original cover image \(x_{j,k}\) and its corresponding stego image. When data is embedded in the \(K^{th}\) significant bit plane, the worst case PSNR is given by:

\[
PSNR = 10 \log_{10} \frac{255^2}{(2^K - 1)^2} dB
\]  

(3)

Eqn. 3 testifies the fact that higher the significant bit plane chosen for embedding data, worst the PSNR, and hence poor perceptual quality of image. Thus, when data is embedded in the higher order planes there is a need for pixel adjustment so as to ensure a better quality stego image. The pixel adjustment algorithm is discussed below.

**Pixel adjustment algorithm**

The process of data embedding and PEPA, as required for such embedding is summarized as under:

i. A test image of size \(P \times Q\) is converted into a row vector of size \((1, P \times Q)\)

ii. An embedding location pointer (PAV) capable of addressing all the pixels is generated.

iii. The secret data is scrambled and embedded in 3rd ISB plane of cover image at the locations pointed to by the respective PAV addresses.

iv. When the embedded data bit \(d_i\) is same as that of the selected location \(b_i\) for data embedding then no pixel adjustment is required.

v. In case the embedded data bit \(d_i\) is 1 and cover image bit at the selected location \(b_i\) is 0, then replace the three lower significant bits of the pixel under consideration are replaced by 0’s (000).
vi. When the bit to be embedded $d_i$ is 0 and is not equal to the data bit $b_i$ at the selected location for data embedding, the lower three significant bits of the concerned pixel are replaced by 1’s (111).

**Results and Discussions**

Various test images of size 256×256 have been used in the proposed system to test the efficacy of the proposed scheme. Various image indices like Peak Signal to Noise Ratio (PSNR), Normalized Absolute Error (NAE), and Normalized Cross Correlations (NCC) have been calculated. If $x_{ij,k}$ and $x'_{ij,k}$ respectively represent host image and its corresponding stego version then NAE and NCC are calculated as follows:

$$\text{NAE} = \frac{\sum_{j=1}^{M} \sum_{k=1}^{N} |x_{ij,k} - x'_{ij,k}|}{\sum_{j=1}^{M} \sum_{k=1}^{N} |x_{ij,k}|}$$  \hspace{1cm} (4)

$$\text{NCC} = \frac{\sum_{j=1}^{M} \sum_{k=1}^{N} x_{ij,k} * x'_{ij,k}}{\sum_{j=1}^{M} \sum_{k=1}^{N} x_{ij,k}^2}$$  \hspace{1cm} (5)

$M$ and $N$ are number of pixels in row and column directions, respectively.

The proposed technique provides a two layer security to the embedded data. Firstly, data is made secure with the help of data scrambler using a secret key. Further, another layer of data security is added by embedding data at pseudorandom locations in the cover image. The proposed technique has been compared with that reported in [12] for a payload of 500 bytes of data as shown in Table 1. The comparison results show that besides providing additional layer of security to the embedded data, the proposed scheme also enhances PSNR by about 3dB and as such provides a better stego-image quality. Fig. 2 shows the various cover images with corresponding stego images for a payload of 32786 bits. Figures 3 and 4 show the comparison results of the proposed technique with that reported by Singh *et.al* [12] for various image quality indices. Further, as can be observed from the tabulated values, NCC in most of the cases is equal to unity or very near to unity, indicating that stego-image is very close in perception to the original cover image.
Table 1 Comparison between proposed technique and [12]

<table>
<thead>
<tr>
<th>Test Image</th>
<th>Embedded data Size in Bytes</th>
<th>PSNR (dB)</th>
<th>NCC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Singh et. al</td>
<td>Proposed</td>
<td>Singh et. al</td>
</tr>
<tr>
<td>Lena</td>
<td>500</td>
<td>512</td>
<td>49.01</td>
</tr>
<tr>
<td>Goldhill</td>
<td>500</td>
<td>512</td>
<td>49.45</td>
</tr>
<tr>
<td>Mandrill</td>
<td>500</td>
<td>512</td>
<td>49.23</td>
</tr>
<tr>
<td>Cameraman</td>
<td>500</td>
<td>512</td>
<td>48.72</td>
</tr>
</tbody>
</table>

Fig. 2 Cover images and corresponding stego-images for payload of 32786 bits
Conclusion

A secure data hiding technique that embeds data in Intermediate Significant Bit (ISB) plane of cover images has been presented. The security of embedded data has been taken care of, by scrambling it prior to embedding. Further, the scrambled secret data has been pseudorandomly embedded in the cover image to add one more layer of data security. The adversary, as such, needs two different keys to break the system, one used for data encryption and the other used for pseudorandom address vector generation. To improve the stego-image quality the data embedding is followed by Pixel adjustment algorithm. Image quality indices like PSNR, NCC, and NAE have been calculated for evaluating the efficiency of the proposed technique. The proposed technique has been compared with that reported by Sing et.al [18] for a payload of 500 bytes of data. It is evident from the comparison
Table that, besides providing an additional layer of security, the proposed technique provides an improvement in PSNR and NCC even though a slightly more data is embedded in various test images, an indication of the fact that the proposed technique is capable of producing quality stego images. ISB embedding further ensures non-vulnerability of the proposed technique to LSB removal/replacement attack.

References