LSB Matching Revisited

Jarno Mielikainen, Member, IEEE

Abstract

This letter proposes a modification to the Least-Significant-Bit (LSB) matching, a steganographic method for embedding message bits into a still image. In the LSB matching the choice of whether to add or subtract one from the cover image pixel is random. The new method uses the choice to set a binary function of two cover pixels to the desired value. The value of the binary function is used to carry information. Therefore, the modified method allows embedding the same payload as LSB matching, but with fewer changes to the cover image.

Index Terms

Information hiding, steganography.

I. INTRODUCTION

Steganography is an application of information hiding. Generally a good steganographic technique should have good visual/statistical imperceptibility and a sufficient payload [1]. The proposed method is a modified version of the Least-Significant-Bit (LSB) method, resulting in improved imperceptibility.

LSB replacement embeds a message into the cover image by replacing the LSBs of the cover image with message bits to arrive at the stego image. The method increases even pixel values either by one or leaves them unmodified, while odd values are left unchanged or decreased by one. Due to imbalance in the embedding distortion, LSB replacement can be detected by the current detection methods [2] - [6].

LSB matching also modifies the LSBs of the cover image for message embedding. LSB matching does not simply replace the LSBs of the cover image as LSB replacement does. Instead, if the message bit does not match the LSB of the cover image, then one is randomly either added or subtracted from the value of the cover pixel. To ensure the invertibility of the process, pixel values are never modified to fall outside of the allowable range [7].

Only a few detection methods for LSB matching have been proposed [8] - [11]. The best known detector for LSB matching is based on the center of mass (COM) of the histogram characteristic function (HCF) introduced by Harmsen et al. [12]. Ker [8] improved the detection rates for gray-scale images by using a down-sampled image for calibration. He also proposed using the adjacency histogram instead of the usual histogram.

Manuscript submitted October 6, 2005. This work was supported by the Academy of Finland.

J. Mielikainen is with the Department of Information Technology, Lappeenranta University of Technology, 53851 Lappeenranta, Finland.

e-mail: mielikai@lut.fi.

phone: +1 805 322 7289.

draft: +358 5 621 2899.
Our proposed method allows an embedding of the same amount of information as LSB matching, but with fewer changes to the cover image. This makes the detection of our method harder than the conventional LSB matching method.

II. PROPOSED METHOD

The proposed method uses gray-scale cover images. The message embedding is performed for the two cover image pixels at a time. Gray-level values of those two pixels are \(x_i\) and \(x_{i+1}\).

After the message embedding, value of the \(i\)th message bit, \(m_i\), is equal to the LSB of stego image’s \(i\)th pixel, \(y_i\). Value of the \(i+1\)th message bit, \(m_{i+1}\), is a function of \(y_i\) and \(y_{i+1}\).

The proposed method allows a selection of addition/subtraction of \(y_i\) to carry information, because the selection can set a binary function \(f(y_i, y_{i+1})\) to the desired value. If a binary function has the following two properties,

\[
\begin{align*}
    f(y_i, y_{i+1}) &= f(y_i + 1, y_{i+1}) \\
    f(y_i, y_{i+1}) &\neq f(y_i - 1, y_{i+1}),
\end{align*}
\]

then a controlled change of the value of \(y_i\) by one allows the setting of \(f(y_i, y_{i+1})\) to the desired value. If a binary function \(f(y_i, y_{i+1})\) is of the form

\[
f(y_i, y_{i+1}) \neq f(y_i, y_{i+1} + 1),
\]

then both an increase and a decrease of \(y_{i+1}\) by one will change the value of the function \(f(y_i, y_{i+1})\). The function \(f(y_i, y_{i+1}) = \text{LSB}(\lfloor y_i/2 \rfloor + y_{i+1})\) has the properties of Equations (1)-(3).

The embedding algorithm first compares the LSB of \(x_i\) to \(m_i\). If they are not equal, then \(y_{i+1}\) is set to \(x_{i+1}\) and a comparison between \(f(x_i - 1, x_{i+1})\) and \(m_{i+1}\) is performed. If comparison is true, then \(y_i\) is set to \(x_i - 1\), so that \(f(y_i, y_{i+1}) = m_{i+1}\). Otherwise, the value of \(y_i\) is set to \(x_i + 1\).

If the LSB of \(x_i\) is equal to the message bit \(m_i\), then \(y_i = x_i\) and \(f(x_i, x_{i+1})\) is compared to the message bit \(m_{i+1}\). If they are not equal, then \(y_{i+1} = x_{i+1} \pm 1\) would make \(f(y_i, y_{i+1}) = m_{i+1}\). The choice of whether to add or subtract one from \(x_{i+1}\) is performed separately both for the even and odd valued regions. The even and odd valued regions refer to the areas of the cover image were the pixel values are even and odd, respectively. Inside both regions, the increment/decrement selection is made to minimize the sum of the absolute differences between the cover image and the stego image. The selection thus avoids the LSB replacement style imbalance.

The expected number of modifications per pixel can be computed using,

\[
P(x_i \neq m_i) + P(x_i = m_i)P(f(x_i, x_{i+1}) \neq m_{i+1})/2,
\]

where \(P()\) is the probability function. If ones and zeros are equally likely both in the message and in the LSBs of the cover image, then \(P(x_i \neq m_i) = P(x_i = m_i) = P(f(x_i, x_{i+1}) = m_{i+1}) = 0.5\). Therefore, the expected number of modifications per pixel is 0.375. The message embedding order is determined by the same pseudo-random sequence generator as in LSB matching [7].
III. EXPERIMENTAL RESULTS

One thousand JPEG images [13], all sized 384 × 256, were used in our experiments. JPEG images were used as the cover images, because the HCF COM detectors work best on them [8]. The images were converted to gray-scale before use. The cover images were embedded with maximal-length random messages, such as messages obtained by encryption.

On average, LSB matching and the new method required 0.500 and 0.375 modifications per pixel, respectively. The experimental results agree with the theoretical results.

Also, the absolute values of the sum of differences per pixel between the cover and stego image for the even and odd regions were computed. These experiments were used to determine if the new method exhibits bias. For both regions, the average results were 0.500 and 0.000 for LSB replacement and the new method, respectively. The results confirm that the new method does not have LSB replacement style imbalance.

Fig. 1 depicts receiver operating characteristic (ROC) curves using the calibrated HCF COM for message detection. The curves show how the probability of detection and probability of false positive vary as the detection threshold is adjusted. Similarity, in Fig. 2, ROC curves for the calibrated adjacency HCF COM are given.

From the ROC curves it can be seen that the novel embedding algorithm decreases the probability of detection for the HCF COM detectors compared to LSB matching.

IV. CONCLUSIONS

The proposed steganographic method allows an embedding of the same amount of information into the stego image as LSB matching. At the same time, the number of changed pixel values is smaller. The proposed method does not have the asymmetric property of LSB replacement method. Therefore, it is immune against steganographic
attacks that utilize the asymmetric property. Finally, the detection of the existence of the hidden messages using the HCF COM based detectors is less efficient against the method compared to LSB matching.

ACKNOWLEDGMENT

The author would like to thank Professor Sanjit K. Mitra who took the time to carefully review the letter.

REFERENCES
