Journal of Computer Applications (JCA)
ISSN: 0974-1925, Volume IV, Issue 1, 2011

Edge Adaptive Image Steganography Based On LSB Matching Revisited

[1]Mrs. Sivaranjani [2]Ms. Semi Sara mani

Abstract— **The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those images with many smooth regions. In this paper, we expand the LSB matching revisited image steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. Keywords-**

Index Terms — **Content-based steganography, least-significant-bit (LSB)-based steganography, pixel-value differencing (PVD), security, steganalysis.**

I. INTRODUCTION

STEGANOGRAPHY is a technique for information hiding. It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious. On the other side, steganalysis aims to expose the presence of hidden secret messages in those stego media. If there exists a steganalytic algorithm which can guess whether a given media is a cover or not with a higher probability than random guessing, the steganographic system is considered broken. In this paper, we consider digital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain. LSB replacement is a well-known steganographic method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms.

Manuscript received May 14, 2011.

Mrs. Sivaranjani[1], Department of Computer Science and Engineering, Avinashlingam Deemed University for Women, Coimbatore.
Ms. Semi Sara mani[2], PG scholar, Department of information technology, Easa College of engineering & technology, Coimbatore.

LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the
cover image, then or is randomly added to the corresponding pixel value. Statistically, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry artifacts introduced by LSB replacement can be easily avoided. Therefore, the common approaches used to detect LSB replacement are totally ineffective at detecting the LSBM. Up to now, several steganalytic algorithms (e.g., [7]–[10]) have been proposed to analyze the LSBM scheme. Unlike LSB replacement and LSBM, which deal with the pixel values independently, LSB matching revisited (LSBMR) [1] uses a pair of pixels as an embedding unit, in which the LSB of the first pixel carries one bit of secret message, and the relationship (odd–even combination) of the two pixel values carries another bit of secret message. In such a way, the modification rate of pixels can decrease from 0.5 to 0.375 bits/pixel (bpp) in the case of a maximum embedding rate, meaning fewer changes to the cover image at the same payload compared to LSB replacement and LSBM. It is also shown that such a new scheme can avoid the LSB replacement style asymmetry, and thus it should make the detection slightly more difficult than the LSBM approach based on our experiments. The typical LSB-based approaches, including LSB replacement, LSBM, and LSBMR, deal with each given pixel/pixel pair without considering the difference between the pixel and its neighbors. The pixel-value differencing (PVD)-based scheme (e.g., [17]–[19]) is another kind of edge adaptive scheme, in which the number of embedded bits is determined by the difference between a pixel and its neighbor. The larger the difference, the larger the number of secret bits that can be embedded. Usually, PVD-based approaches can provide a larger embedding capacity. Assuming that a cover image is made up of many no overlapping small sub images (regions) based on a predetermined rule, then different regions usually have different capacities for hiding the message. Generally, the regions located at the sharper edges present more complicated statistical features and are highly dependent on the image contents. In this paper, we propose an edge adaptive scheme and apply it to the LSBMR-based method. The rest of the paper is arranged as follows. Section II analyzes the limitations of the relevant steganography schemes and proposes some strategies. Section III shows the details of data embedding and data extraction in our scheme. Section IV presents experimental results and discussions. Finally, concluding remarks and future.

II. PROPOSED SCHEME

The flow diagram of our proposed scheme is illustrated in Fig. 4. In the data embedding stage, the scheme first initializes some parameters, which are used for subsequent

data preprocessing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message, then data hiding is performed on the selected regions. Finally, it does some post processing to obtain the stego image. Otherwise the scheme needs to revise the Parameters, and then repeats region selection

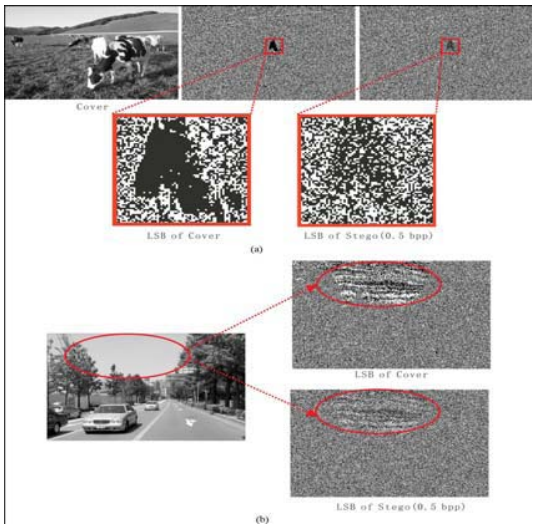

Figure 1.

and capacity estimation until can be embedded completely. Please note that the parameters may be different for different image content and secret message. In data extraction, the scheme first extracts the side information from the stego image. Based on the side information, it then does some preprocessing and identifies the regions that have been used for data hiding. Finally, it obtains the secret message according to the corresponding extraction algorithm. In this paper, we apply such a region adaptive scheme to the spatial LSB domain. We use the absolute difference between two adjacent pixels as the criterion for region selection, and use LSBMR as the data hiding algorithm. The details of the data embedding and data extraction algorithms are as follows.

A. Data Embedding

Step 1: The cover image of size of is first divided into non overlapping blocks of pixels. For each small block, we rotate it by a random degree in the range of, as determined by a secret key. The resulting image is rearranged as a row vector by raster scanning. And then the vector is divided into non overlapping embedding units with every two consecutive pixels, where, assuming is an even number. Two benefits can be obtained by the random rotation. First, it can prevent the detector from getting the correct embedding units without the rotation key, and thus security is improved. Furthermore, both horizontal and vertical edges (pixel pairs) within the cover image can be used for data hiding.

Step 2: According to the scheme of LSBMR, 2 secret bits can be embedded into each embedding unit. Therefore, for a given secret message, the threshold for region selection can be determined as follows. Let be the set of pixel pairs whose absolute differences are greater than or equal to a parameter t

$$EU(t) = \{(x_i, x_{i+1}) \mid |x_i - x_{i+1}| \geq t, \forall (x_i, x_{i+1}) \in V\}$$

Then we calculate the threshold T by

$$T = \arg^{max}_{i}\{2 \times |EU(t)| \geq |M|\}$$

where, is the size of the secret message , and denotes the total number of elements in the set of .

Step 3: Performing data hiding on the set of

$$\mathbf{EU(T)}=\{(x_i, x_{i+1}) \mid |x_i - x_{i+1}| \geq T, \forall (x_i, x_{i+1}) \in V$$

We deal with the above embedding units in a pseudorandom order determined by a secret key . For each unit , we perform the data hiding according to the following four cases.

Case #1:

$$\mathbf{LSB}(x_i) = m_i \,\&\, f(x_i, x_{i+1}) = m_{i+1}$$
$$(x_i', x_{i+1}') = (x_i, x_{i+1});$$

Case #2:

$$\mathbf{LSB}(x_i) = m_i \,\&\, f(x_i, x_{i+1}) \neq m_{i+1}$$
$$(x_i', x_{i+1}') = (x_i, x_{i+1} + \mathbf{r});$$

Case#3:

$$\mathbf{LSB}(x_i) \neq m_i \,\&\, f(x_i - 1, x_{i+1}) = m_{i+1}$$
$$(x_i', x_{i+1}') = (x_i - 1, x_{i+1});$$

Case # 4:

$$\mathbf{LSB}(x_i) \neq m_i \,\&\, f(x_i - 1, x_{i+1}) \neq m_{i+1}$$
$$(x_i', x_{i+1}') = (x_i + 1, x_{i+1});$$

where and denote two secret bits to be embedded. The function is defined as . is a random value in and denotes thepixel pair after data hiding. After the above modifications, and may be out of , or the new difference may be less than the threshold . In such cases,1 we need to readjust them as

$$(x_i'' , x_{i+1}'' \text{)by } (x_i'' , x_{i+1}'' \text{)=arg } min_{(e1,e2)}\{|e_1 - x_i| + |e_2 - x_{i+1}| | e_1 = x_i' + 4k_1', e_2 = x_{i+1}' + 2k_2, |e_1 - e_2| \geq T, 0 \leq e_1, e_2 \leq 255, 0 \leq T \leq 31, k_1, k_2 \in Z\}. (*)$$

Finally, we have

$$LSB(x_i'') = m_i, f((x_i'', x_{i+1}'') = m_{i+1}$$

Step 4: After data hiding, the resulting image is divided into non overlapping blocks. The blocks are then rotated by a random number of degrees based on. The process is very similar to **Step 1** except that the random degrees are opposite. Then we embed the two parameters into a preset region which has not been used for data hiding. The first one is the block size for block dividing in data preprocessing; another is the threshold for embedding region selection. In all, only 7 bits of side information are needed for each image.

III. CONCLUDING REMARKS

In this paper, an edge adaptive image steganographic scheme in the spatial LSB domain is studied. As pointed out in Section II, there usually exist some smooth regions in natural images, which would cause the LSB of cover images not to

be completely random or even to contain some texture information just like those in higher bit planes. If embedding a message in these regions, the LSB of stego images becomes more random, and according to our analysis and extensive experiments, it is easier to detect. In most previous steganographic schemes, however, the pixel/pixel-pair selection is mainly determined by a PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that those smooth/flat regions will be also contaminated by such a random selection scheme even if there are many available edge regions with good hiding characteristics. To preserve the statistical and visual features in cover images, we have proposed a novel scheme which can first embed the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges.. Furthermore, it is expected that our adaptive idea can be extended to other steganographic methods such as audio/video steganography in the spatial or frequency domains when the embedding rate is less than the maximal amount.

REFERENCES

[1] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.
[2] A.Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Proc. 3rd Int. Workshop on Information Hiding, 1999, vol. 1768, pp. 61–76.
[3] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," IEEE Multimedia, vol. 8, no. 4, pp. 22–28, Oct. 2001.
[4] S. Dumitrescu, X.Wu, and Z.Wang, "Detection of LSB steganography via sample pair analysis," IEEE Trans. Signal Process., vol. 51, no. 7, pp. 1995–2007, Jul. 2003.
[5] A.D. Ker, "A general framework for structural steganalysis of LSB replacement," in Proc. 7th Int. Workshop on Information Hiding, 2005, vol. 3427, pp. 296–311.
[6] D. Ker, "A funsion of maximum likelihood and structural steganalysis," in Proc. 9th Int. Workshop on Information Hiding, 2007, vol. 4567, pp. 204–219.
[7] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," Proc. SPIE Electronic Imaging, vol. 5020, pp. 131–142, 2003.
[8] A.D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.
[9] F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels," in Proc. IEEE Int. Conf. Image Processing, Oct. 16–19, 2007, vol. 1, pp. 401–404.
[10] X. Li, T. Zeng, and B. Yang, "Detecting LSB matching by applying calibration technique for difference image," in Proc. 10th ACM Workshop on Multimedia and Security, Oxford, U.K., 2008, pp. 133–138.
[11] Y. Q. Shi et al., "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 6–8, 2005, pp. 269–272.
[12] Li, J. Huang, and Y. Q. Shi, "Textural features based universal steganalysis," Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia, vol. 6819, p. 681912, 2008.
[13] M. Goljan, J. Fridrich, and T. Holotyak, "Newblind steganalysis and its implications," Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia, vol. 6072, pp. 1–13, 2006.
[14] K. Hempstalk, "Hiding behind corners: Using edges in images for better Steganography," in Proc. Computing Women's Congress, Hamilton, New Zealand, 2006.
[15] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image," in Proc. Int. Conf. Information and Communication Technology, Mar. 2007, pp. 238–241.
[16] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," in Proc. IEEE on Digital Signal Processing Workshop, Sep. 1996, pp. 37–40.
[17] Wu and W. Tsai, "A steganographic method for images by pixelvalue differencing," Pattern Recognit. Lett., vol. 24, pp. 1613–1626, 2003.
[18] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," Pattern Recognit. Lett., vol. 25, pp. 331–339, 2004.
[19] H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497, Sep. 2008.
[20] M. Kharrazi, H. T. Sencar, and N. Memon, "Cover selection for steganographic embedding," in Proc. IEEE Int. Conf. Image Processing, Oct. 8–11, 2006, pp. 117–120.

BIOGRAPHY

Simi Sara Mani graduated from Karunya University, in information technology during the year 2008. She obtained her Master degree in Computer Science and Engineering from Faculty of Engineering, Avinashlingam Deemed University for Women, Coimbatore in the year 2011. At present she is a lecturer in the Department of Computer Science and Engineering, Easa College of engineering & technology, Coimbatore, India. Her area of interest includes Data mining and Web Services. She has 1 year of experience in teaching.

S. Sivaranjani graduated from Anna University, in Computer Science and Engineering during the year 2005. She obtained her Master degree in Computer Science and Engineering from Anna University of Technology, Coimbatore in the year 2010. At present she is an assistant professor in the Department of Computer Science and Engineering, Faculty of Engineering, Avinashlingam Deemed University for Women, Coimbatore, India. Her area of interest includes Data mining and Web Services. She has 5 years of experience in teaching.