Image Steganography Using Cross Paired Edge Adaptive *LSB* Matching Revisited

Gawade Sushil S.
Terna Engineering College
Nerul, Navi Mumbai, India
gawade.sushil@gmail.com

Gaikwad V. B.
Terna Engineering College
Nerul, Navi Mumbai, India
vb_2k@rediffmail.com

ABSTRACT

Steganography is the art and science of writing hidden messages in such a way that nobody with the exception of the sender and meant recipient, even realizes there is a hidden message. However, in most existing approaches, the selection of embedding positions among a cover image principally depends on a pseudorandom number generator while not considering the relationship between the image content itself and also the size of the secret message. Hence the smooth or flat regions within the cover pictures can inevitably be contaminated when hiding an information even at a low embedding rate and this can cause poor visual quality and low security, particularly for those pictures with several smooth regions. Here, LSB matching revisited image steganography is planned with a cross pair edge adaptive theme which may choose the embedding regions in line with the size of secret message and also the difference between two consecutive pixels within the cover image. In this letter, the authors point out the reduced effect of B-spline curve fitting introduced in original method.

1. INTRODUCTION

On the premise of cover object, steganography is also of the many sorts like image, audio, video steganography etc. Image Steganography is extremely widespread because of popularity of digital image transmission over the web. Image Steganography use redundancy of digital image to cover the key information. It should be divided into two classes. They are spatial domain strategies and frequency domain ones. In the spatial domain, the secret messages are embedded within the image pixels directly. In the frequency domain, however, the cover image is initially transformed to frequency domain, so the messages are embedded within the transformed.

LSB replacement is a well-known steganographic technique. During this embedding method, solely the LSB plane of the cover image is overwritten with the secret bit stream as per a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels once concealing the data) is introduced and so it is very simple to notice the existence of hidden message even at a low embedding rate. LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then +1 or -1 is randomly added to the corresponding pixel value. Statistically, the chance of increasing or decreasing for every changed pixel value is the same and then the obvious asymmetry artifacts introduced by LSB replacement may be simply avoided. Therefore, the common approaches used to discover LSB replacement are entirely ineffective at detecting the LSBM.

Unlike LSB replacement and LSBM, that handle the pixel values independently, LSB matching revisited (LSBMR) uses a pair of pixels as an embedding unit, within 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 the way, the modification rate of pixels will decrease from 0.5 to 0.375 bits/pixel (bpp) in the case of a most embedding rate, which means fewer changes to the cover image at an equivalent payload compared to LSB replacement and LSBM. It is also shown that such a replacement method will avoid the LSB replacement style asymmetry and so it ought to make the detection slightly harder than the LSBM. The standard LSB based approaches like LSB replacement, LSBM and LSBMR deal with every given pixel/pixelpair while not considering the difference between the pixel and its neighbours. Until now, many edge adaptive schemes are investigated. Concealing data at edges is safer against visual attack and therefore provides additional security than embedding at random locations. The pixel value differencing (PVD) based theme [5]-[7] is another kind of edge adaptive theme, within which the number of embedded bits is decided by the difference between a pixel and its neighbour. The larger the difference, the larger the quantity of secret bits which will be embedded. Usually, PVD based approaches will offer a bigger embedding capability (on average, larger than 1 bpp), but cannot make full use of edge information for data hiding and that they are poor at resisting some statistical analyses.

One of the common characteristics of most of the steganographic strategies mentioned above is that the pixel/pixelpair choice is principally determined by a PRNG whereas neglecting the relationship between the image content and also the size of the secret message. By doing this, these strategies will spread the secret information over the total stego image at random even at low embedding rate. However, it is seen that such embedding schemes do not perform well in

ICCCNT '16, July 06-08, 2016, Dallas, TX, USA
© 2016 ACM. ISBN 978-1-4503-4179-0/16/07…$15.00
DOI: http://dx.doi.org/10.1145/2967878.2973277

terms of the security or visual quality of the stego images. Generally, the regions located at the sharper edges provide additional complicated statistical features and are extremely dependent on the image contents. Moreover, it is tougher to observe changes at the sharper edges than those in flat regions.

The Edge Adaptive LSB Matching Revisited (EALSBMR) technology proposed by Luo et al. [1] is strong method of spatial domain image steganography which is region adaptive improved LSB Matching Revisited. This method performs embedding at lower pixel modification rate and uses smooth area within cover image only if required. As per Tan et al. [9] there is no targeted steganalysis against EALSBMR, except B-spline curve fitting.

There are certain properties of strong steganography. In order to avoid being the suspicious, the hidden contents should be invisible both perceptually and statistically. Steganography techniques ought to produce high imperceptible Stego-image. Unlike watermarking, that has to embed solely a small quantity of copyright data, steganography aims at hidden communication and so usually requires sufficient embedding capability. Requirements for higher payload and secure communication are typically contradictory. Counting on the precise application scenarios, a tradeoff needs to be sought. Stego image should provide robustness to image processing techniques like compression, cropping, resizing etc. i.e. when any of these techniques are performed on stego image, secret information should not be destroyed completely.

There is no technique of steganography which provide all the three properties at high level. There is a trade-off between the capacity of the embedded data and the robustness to certain attacks, while keeping the perceptual quality of the stego-medium at an acceptable level. It is not possible to attain high robustness to signal modifications and high insertion capacity at the same time[8].

2. ANALYSIS OF LIMITATIONS OF RELEVANT APPROACHES AND STRATEGIES

There are typical LSB based approaches including LSB replacement, LSBM and LSBMR, with some adaptive schemes including the PVD scheme [5], adaptive edges with LSB (AE-LSB) [7] and hiding behind corners (HBC) [3].

2.1 LSB Based Methods

In any image higher significant bits carry most of the pixel data and any modification made to those bits will turn out large difference in pixel value. Therefore these bits are always kept untouched, however lower significant bits do not cause significant modification in pixel value and may be used to carry our secret information. This property of LSB is employed in several of the steganographic strategies and therefore those are referred to as LSB based strategies. Here we shall be discussing few of these briefly.

For LSB replacement which is the most well-liked technique amongst all LSB techniques, the secret bit simply overwrites the LSB of the pixel, i.e., the first bit plane, whereas the upper bit planes (2 to 8) are preserved, thus at the time of retrieval solely LSB of stego image is extracted to regenerate secret message. For the LSB Matching method, if the secret bit is not equal to the LSB of the given pixel, then +1or -1 is added randomly to the pixel whereas keeping the altered pixel within the range of [0,255]. In such a way, the LSB of pixels on the traveling order can match the secret bit stream after information hiding both for LSB replacement and LSBM. Therefore, the extracting method is exactly a similar for the two approaches. It first generates a similar traveling order as per a shared key, then the hidden message will be extracted properly by checking the parity bit of pixel values.

LSBMR applies a pixel pair (x_i, x_{i+1}) within the cover image as an embedding unit rather than single pixel at a time. after message embedding, the unit is changed as (x'_i, x'_{i+1}) within the stego image that satisfies $LSB(x'_i) = m_i, LSB(\lfloor x'_i/2 \rfloor + x'_{i+1}) = m_{i+1}$, where the function $LSB(x)$ denotes the LSB of the pixel value x. m_i and m_{i+1} are the two secret bits to be embedded.

By using the relationship (odd-even combination) of adjacent pixels, the modification rate of pixels in LSBMR would decrease compared with LSB replacement and LSBM at identical embedding rate. What is additional, it does not introduce the LSB replacement style asymmetry. Similarly, in information extraction, it first generates a traveling order by a PRNG with a shared key. Then for every embedding unit on the order, two bits can be extracted. The first secret bit is that the LSB of the first pixel value and the second bit can be obtained by calculating the relationship between the two pixels as shown above.

2.2 Edge Based Methods

Our human vision is sensitive to slight changes within the flat regions, whereas it will tolerate a lot of severe changes within the edge regions. Therefore changes made in pixels at edges introduce very less visual artifacts. Many pixel value Differencing (PVD) based strategies like [5]-[7] are planned to enhance the embedding capability while not introducing obvious visual artifacts into the stego pictures.

The basic idea of PVD based approaches is to first divide the cover image into several non-overlapping units with two consecutive pixels then handle the embedding unit on a pseudorandom order that is also decided by a PRNG. The larger the difference between the two pixels, the larger the quantity of secret bits that may be embedded in the unit. To some extent, existing PVD based approaches are edge adaptive since a lot of secret information is embedded in those busy regions. However, almost like the LSBM and LSBMR approaches, pixel selection choice is especially dependent on a PRNG, which suggests that the changed pixels can still be spread around the whole stego image, whereas several available sharp edge regions have not been fully exploited.

Most existing steganographic approaches sometimes assume that the LSB of natural covers is insignificant and random enough and therefore those pixels/pixel pairs for information hiding is chosen freely employing a PRNG. However, such an assumption is not always true, particularly for pictures with several smooth regions. It is clearly observed that the LSB will reflect the texture data of the cover image to some extent. Compared with smooth regions, the LSB of pixels located in edge regions sometimes present a lot of random characteristics, and that they are statistically like the distribution of the secret message bits (assuming a 1/0 uniform distribution). Therefore, it is expected that fewer detectable artifacts and visual artifacts would be left within the edge regions after information hiding. Moreover, the edge information (such as the location and also the statistical moments) is extremely dependent on image content, which can make detection even harder. This is often why this method can first embed the secret bits into edge regions as far as potential whereas keeping different smooth regions as they are. HBC technique [3] has this property. However, the HBC technique simply modifies the LSBs whereas keeping the most significant bits unchanged. Therefore it is considered an edge adaptive case of LSB replacement, and also the LSB replacement style imbalance will also occur in their stego.

To a definite extent, existing PVD-based approaches are edge adaptive since additional secret information is embedded in those busy regions. However, almost like the LSBM and LSBMR approaches, pixel pair choice is especially dependent on a PRNG, which implies that the modiïňĄed pixels can still be spread around the whole stego image and plenty of smooth regions are going to be altered inevitably when concealing an information even if the difference between two consecutive pixels is zero, whereas several available sharp edge regions have not been fully exploited.

Hence, there typically exists some smooth regions in natural pictures, which might cause the LSB of cover pictures to not be completely random or perhaps to contain some texture data just like those in higher bit planes. If embedding a message in these regions, the LSB of stego pictures becomes more random, and it is easier to sight. In most previous steganographic schemes, however, the pixel/pixel-pair choice is principally determined by a PRNG while not considering the connection between the characteristics of content regions and therefore the size of the secret message to be embedded, which implies that those smooth/flat regions are also contaminated by such a random choice scheme even if there are several available edge regions with good concealing characteristics.

Hence, we need such a strong steganographic method that reduces pixel modification ratio even at high embedding rates and avoids random embedding of data in cover images. EALSBMR [1] does the same which is required, but it is vulnerable to B-spline fitting technique [9].

3. CROSS PAIR EALSBMR ALGORITHM

We propose a scheme that enhance original EALSBMR to resist B-spline fitting. The scheme first initializes few parameters, which are used for subsequent data preprocessing and region selection, and then derives the capacity of those selected regions.

In this method, we adapt EALSBMR as the information hiding algorithm. The details of the data embedding and extraction algorithms are explained further.

3.1 Data Embedding Process

Step 1 :The cover image I of size of $m \times n$ is first divided into non overlapping blocks of $Bz \times Bz$ pixels. For each small block, We rotate it by a random degree in the range of 0, 90, 180, 270 as determined by a secret key. The resulting image is then divided into non overlapping embedding units with every two consecutive pixels (x_i, x_{i+1}), where $i = 1, 3, 5, .., mn$ assuming n 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 M, the threshold T for region selection can be determined as follows. Let $E(t)$ be the set of pixel pairs whose absolute differences are greater than or equal to a parameter t,

$$E(t) = \{(x_i, x_{i+1}) \mid\mid (x_i - x_{i+1}) \mid\geq t, \forall (x_i, x_{i+1}) \in I\} \tag{1}$$

Then calculate the threshold by

$$T = \arg\max\{2 \times EU(T) \geq\mid M \mid\} \tag{2}$$

When $T = 0$ the method becomes the conventional LSBMR scheme, which means that our method can achieve the same payload capacity as LSBMR (except for 5 bits).

Step 3 :First threshold and then data hiding is performed on the set of

$$E(T) = \{(x_i, x_{i+1}) \mid\mid (x_i - x_{i+1}) \mid\geq T, \forall (x_i, x_{i+1}) \in I\} \tag{3}$$

Here we are dealing with two pixel pairs as an embedding unit. Consider (a_i, a_{i+1}) is one pair and (b_i, b_{i+1}) is other pair. These pairs are then crossed with each other to form new pairs such as (a_i, b_{i+1}) is one pair and (b_i, a_{i+1}). Two bits are stored in each pair with first bit at LSB of first pixel and second bit as a binary relationship at LSB of second pixel as per following EALSBMR algorithm [1].

Case 1 : $LSB(x_i) = m_i$ & $f(x_i, x_{i+1}) = m_{i+1}$ then $(x'_i, x'_{i+1}) = (x_i, x_{i+1})$

Case 2 : $LSB(x_i) = m_i$ & $f(x_i, x_{i+1}) \neq m_{i+1}$ then $(x'_i, x'_{i+1}) = (x_i, x_{i+1} + r)$

Case 3 : $LSB(x_i) \neq m_i$ & $f(x_i - 1, x_{i+1}) = m_{i+1}$ then $(x'_i, x'_{i+1}) = (x_i - 1, x_{i+1})$

Case 4 : $LSB(x_i) \neq m_i$ & $f(x_i - 1, x_{i+1}) \neq m_{i+1}$ then $(x'_i, x'_{i+1}) = (x_i + 1, x_{i+1})$

where m_i and m_{i+1} denote two secret bits to be embedded. The function f is defined as

$$f(a, b) = LSB(\lfloor a/2 \rfloor + b) \tag{4}$$

and r is a random value in $\{+1, -1\}$ and (x'_i, x'_{i+1}) denotes the pixel pair after data hiding. This algorithm is used twice for two pairs of embedding unit to hide two bits in one pair. After the modification these pairs are rearranged as original pairs for readjustment phase [1] as any pixel may be out of [0,255], or the new difference between pixel pair may be less than the threshold T. In such cases, it is required to readjust them as (x''_i, x''_{i+1}) by,

$$(x''_i, x''_{i+1}) = \arg\min_{(e_1, e_2)}\{\mid e_1 - x_i \mid + \mid e_2 - x_{i+1} \mid\} \tag{5}$$

where, $e_1 = x'_i + 4k_1, e_2 = x'_{i+1} + 2k_2, \mid e_1 - e_2 \mid\geq T, 0 \leq e_1, e_2 \leq 255, 0 \leq T \leq 31, \{k_1, k_2\} \in Z$. 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 $Bz \times Bz$ blocks. The blocks are then rotated by a random number of degrees based on key.

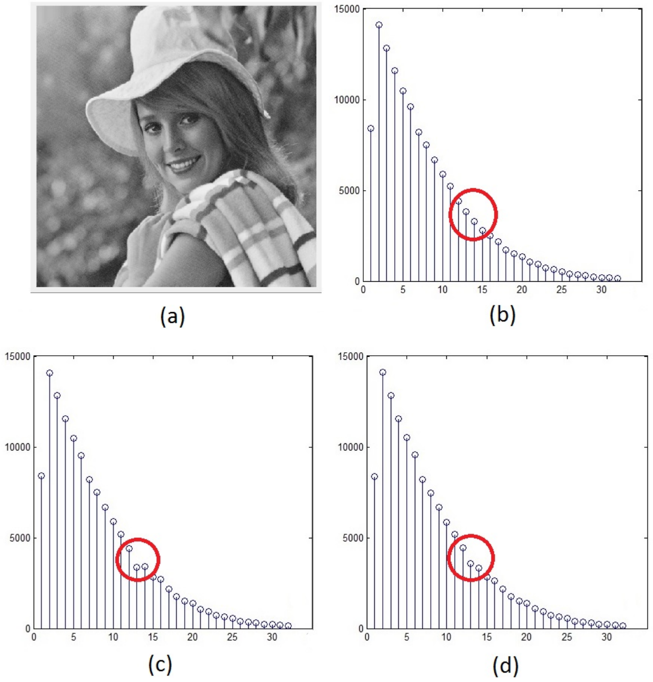

Figure 1: (a) original image (b) HADPP of original image (c) HADPP of original EALSBMR (d) HADPP of proposed cross paired EALSBMR at 10% embedding rate

The process is very similar to Step 1 except that the random degrees are opposite.

3.2 Data Extraction Process

To get data, We first extract the side information, i.e., the threshold T from the stego picture. We then do exactly the same as Step 1 in information embedding. The stego image is divided into $Bz \times Bz$ blocks and the blocks are then rotated by random degrees as per the secret key. Finally, we get the desired embedding units by traveling all the pixel pairs whose absolute differences are more than or equal to the threshold T according to a pseudorandom order based on the secret key, until all the hidden bits are extracted fully. For each qualified embedding unit of two crossed pairs, say (a'_i, b'_{i+1}) and (b'_i, a'_{i+1}), where (a'_i, a'_{i+1}) and (b'_i, b'_{i+1}) are the two original pairs with absolute difference greater that T , the two secret bits extracted from each pair (x'_i, x'_{i+1}) as $m_i = LSB(x'_i)$ and $m_{i+1} = LSB(x'_{i+1})$.

4. EFFECT OF B-SPLINE FITTING

Due to the effect of the EALSBMR readjusting phase pointed out by Tan et al.[9] pulse distortion to the long exponential tail of Histogram of Absolute Difference between Pixel Pairs (HADPP) introduced by EALSBMR readjusting phase put this method vulnerable to attack and a targeted steganalysis method can be implemented which which can detect stego signal. While proposed method reduces the of b-spline fitting (refer fig. 1).

With proposed method we have 0.25 probability that there will be a change at pixel value in both crossed pairs. Further there are half chances that both changes will be at pixels of same original pairs, which lead us to change in threshold after modification to $T-2, T, T+2$. It means with readjustment phase we can put most of these pairs with threshold $T-2$ and $T+2$ back in T with expression in (5) where $k_1 = 0$ and $k_2 = 1$ or -1.

5. CONCLUSION

In most steganographic schemes, the pixel or pixelpair choice is principally determined by a PRNG while not considering the connection between the characteristics of content regions and also the size of the secret message to be embedded, which suggests that those smooth regions are going to be also contaminated by such a random choice scheme even if there are several available edge regions with good concealing characteristics. To preserve the statistical and visual features in cover pictures, projected scheme will adapt EALSBBMR to embed the secret message into the sharper edge regions adaptively according to a threshold determined by the dimensions of the secret message and also the gradients of the content edges. This method will resist to HADPP B-spline fitting introduced through readjustment phase. Resistance will be more for block size greater than one.

6. REFERENCES

[1] Weiqi Luo, Fangjun Huang and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 2, JUNE 2010.*

[2] G.Karthigai Seivi, Leon Mariadhasan, K. L. "Shunmuganathan Steganography Using Edge Adaptive Image", *2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].*

[3] K. Hempstalk, "Hiding behind corners: Using edges in images for better steganography", *in Proc. Computing WomenâĂŹs Congress, Hamilton, New Zealand, 2006.*

[4] 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.*

[5] D. Wu and W. Tsai, "A steganographic method for images by pixel- value differencing," *Pattern Recognit. Lett., vol. 24, pp. 1613-1626, 2003.*

[6] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modiïňĄcation for enhanced security", *Pattern Recognit. Lett., vol. 25, pp. 331-339, 2004.*

[7] C. 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.*

[8] Hong-Juan Zhang, Hong-Jun Tang, "A Novel Image Steganography Algorithm Against Statistical Analysis", *Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.*

[9] Shunquan Tan, "Steganalysis of LSB Matching Revisited for Consecutive Pixels Using B-Spline Functions" , *10th International Workshop on Digital-forensics and Watermarking.*