Adaptive Pixel Swapping Based Steganography Reducing Embedding Noise

Arijit Sur[1], Piyush Goel[2], and Jayanta Mukhopadhyay[2]

[1] Department of Computer Science and Engineering,
Indian Institute of Technology, Guwahati-781039, India
[2] Department of Computer Science and Engineering,
Indian Institute of Technology, Kharagpur-721302, India
arijit@iitg.ernet.in, {piyush,jay}@cse.iitkgp.ernet.in

Abstract. In this paper[1], a block based steganographic algorithm is proposed where embedding is done by swapping two pixels within the block such that resulting additive noise can be adaptively controlled by using a prescribed threshold. The proposed algorithm is used to reduce the extra additive noise which is the main drawback of a existing PSSA algorithm [6]. Regarding the steganographic security, the proposed steganographic scheme inherently preserves first order image statistics such as image histogram and thus remains undetectable against any histogram based spatial domain steganalytic attacks. Experimental results show that the proposed adaptive scheme clearly outperforms the PSSA algorithm [6] against additive noise based blind attacks.

1 Introduction

Steganography is the art of hiding information in an innocent looking cover objects and thus visual and statistical undetectability is one of the major concerns in the steganographic security. In recent steganalytic literature, a major number of algorithms (e.g. [1][2]) are based on first order image statistics. The main problem of restoring image statistics is that an extra amount of additive noise is being added during restoration. This extra additive noise makes those algorithms more vulnerable against additive noise based blind attacks like WAM [3]. It is well known that the chance of detection is substantially reduced if embedding is done adaptively. In this paper, we have consider an existing pixel swapping based spatial domain embedding scheme [6] which can inherently restores image histogram and thus can resist histogram based targeted attacks. The main drawback of the PSSA algorithm [6] is that it essentially adds a substantial amount of extra additive noise due to the restoration process compared to that of LSB matching type of algorithms. In this paper, we have proposed a new *Adaptive Pixel Swapping based Steganographic Algorithm (APSSA)* algorithm by introducing a block based local adaptive threshold such that amount of noise added

[1] The first author gratefully acknowledge the support received from Infosys Technologies Ltd., Bangalore, under the Infosys Fellowship Award.

S.O. Kuznetsov et al. (Eds.): PReMI 2011, LNCS 6744, pp. 299–304, 2011.

(in a block) depends on certain local (within the block) image statistics. It is experimentally shown that proposed scheme has similar performance with PSSA against several recent targeted steganalysis attacks while the proposed adaptive modification made APSSA more secure than PSSA scheme [6] against additive noise based attacks like WAM [3]. The rest of the paper is organized as follows. The proposed encoding and decoding algorithm are described in Sec. 2. In Sec. 3, steganalytic security of the proposed scheme is discussed. The paper will be concluded in Sec. 4.

2 Proposed Scheme

In this paper, a block based pixel swapping algorithm is proposed which is an adaptive improvement over the pixel swapping scheme proposed in [6]. Firstly, the image is divided into non overlapping blocks with a fixed dimension. A single bit is embedded in a block. Let I be the gray scale cover image. Let $I_k(\alpha)$ be the intensity value of a fixed location α in the k^{th} block of the image I. $I_k(\beta)$ and $I_k(\gamma)$ are another two block locations such that β and γ are defined as follows:

$$\beta = argmax_{m \in I_K}(I_K(m) < \mu_k) \tag{1}$$

$$\gamma = argmin_{m \in I_K}(I_K(m) > \mu_k) \tag{2}$$

where $I_K = I_k - I_k(\alpha)$. So $I_k(\beta)$ is a block element other than $I_k(\alpha)$ which is the maximum value just less than μ_k. Similarly $I_k(\gamma)$ is a block element other than $I_k(\alpha)$ having minimum value just greater than μ_k.

The embedding rule is constructed as follows:

$$bit\ embedded = \begin{cases} 1 & \text{if } I_k(\alpha) > \mu_k \\ \\ 0 & \text{if } I_k(\alpha) < \mu_k \end{cases} \tag{3}$$

where μ_k = mean of the k^{th} block. In other words, if $I_k(\alpha)$ is greater than the mean of k^{th} block μ_k, the embedded bit is taken as 1; on the other hand if $I_k(\alpha)$ is less than μ_k, the embedded bit is taken as 0.

A bit is embedded in the k^{th} block if following suitability condition is true for that block

$$|I_k(\alpha) - \mu_k| < \tau \tag{4}$$

where τ is the prescribed threshold.

For a suitable block (say b_k), the present secret bit ($S_{present}$) and $I_k(\alpha)$ are checked according to the embedding rule. If the embedding condition [($S_{present} = 1$) & ($I_k(\alpha) > \mu_k$)] is satisfied, no operation is needed to embed the data bit, otherwise $I_k(\alpha)$ is swapped with $I_k(\beta)$ or $I_k(\gamma)$ according to $S_{present}$. A data bit is embedded if suitability condition is satisfied, otherwise no bit is embedded. In later case, swapping is needed to mark the corresponding block unsuitable for embedding.

This amounts to addition of extra noise. This particular situation happens when both the conditions $|I_k(\alpha) - \mu_k| < \tau$ and $|I_k(\beta) - \mu_k| > \tau$ [or, $|I_k(\alpha) - \mu_k| < \tau$ and $|I_k(\gamma) - \mu_k| > \tau$] are true. It is experimentally found that the probability of occurrences of these situations is very low. This is because $I_k(\beta)$ has the lowest intensity value greater than μ_k of the block and $I_k(\gamma)$ has the highest intensity value less than μ_k of that block. Again for a slightly higher value of τ the situation becomes more rare. Since the total noise added due to this extra swapping is almost negligible, it is not considered in the theoretical computation of noise. There is an obvious trade off between payload and embedding noise. For a relatively higher payload, embedding noise would be relatively high. However when the block size is greater than two, the choice of pixels used for swapping can be possible. This adaptiveness makes the $APSSA$ scheme more secure than $PSSA$ [6] scheme reducing the embedding noise. A step by step algorithm is given below:

2.1 Embedding Algorithm

Algorithm. *Adaptive Pixel Swapping based Steganographic Algorithm (APSSA)*
Input: *Cover Image* I, *Secret Bit Sequence* S, present secret bit is represented by $S_{present}$
Input Parameters: *Shared secret seed for generating pseudorandom sequence*, Threshold (τ)
Output: *Stego Image* I_s

1. The Cover image I is divided into non over lapping blocks of N pixels.
2. Blocks are arranged with a pseudorandom sequence using the shared secret seed.
3. For any block, (let k^{th} block is denoted as I_k), a fixed block location is determined. Let it be denoted by $I_k(\alpha)$. Another two block elements are defined as $I_k(\beta)$ and $I_k(\gamma)$ where $\beta = argmax_{m \in I_K}(I_K(m) < \mu_k)$ and $\gamma = argmin_{m \in I_K}(I_K(m) > \mu_k)$ where μ_k is the mean of the block I_k and $I_K = I_k - I_k(\alpha)$. Let the variable *done* act as a flag denoting, whether the block is used for embedding or not.
4. done = 0

```
if 0 < |I_k(α) − μ_k| < τ
   if ( S_present == 0)
      if I_k(α) > μ_k)
         swap (I_k(α), I_k(β))
         if |(I_k(β) − μ_k)| > τ
            done = 0;
         else
            done = 1;
      else
         done = 1;
```

```
    else
      if I_k(α) < μ_k)
        swap (I_k(α), I_k(γ))
        if |(I_k(γ) − μ_k)| > τ
          done = 0;
        else
          done = 1;
      else
        done = 1;
  if done == 1
    s_present=next secret bit
```

5. Next block is taken and repeat steps 3 and 4 until either the secret sequence (S) is exhausted or all embedding blocks have been used.
6. Using above steps elements of S embedded into I to get stego image I_s.

End. *Adaptive Pixel Swapping based Steganographic Algorithm (APSSA)*

2.2 Extraction Algorithm

The extraction algorithm is quite simple. The pseudorandom sequence of blocks is regenerated at decoder with the help of the shared secret seed. A block (say I_k) is not considered for extraction if $|I_k(\alpha) - \mu_k| \geq \tau$ or $|I_k(\alpha) - \mu_k| = 0$. Otherwise, for any block if $I_k(\alpha) > \mu_k$, the corresponding secret bit is recovered as 1 and 0 if $I_k(\alpha) < \mu_k$. Bit stuffing is used to distinguish between secret sequence and terminator string.

3 Experimental Results

3.1 Reduction of Additive Noise

The main goal of the proposed APSSA scheme is to reduce the additive noise due to the embedding and restoration process of the embedding. In Figure 1, PSNR between cover and stego images are shown for both the PSSA [6] and the APSSA scheme. The experiments are done on 100 randomly chosen images from a never compressed image dataset UCID [4]. In Figure 1, it is observed that the PSNR between cover and stego images of the proposed APSSA scheme is relatively higher than that of PSSA [6] scheme which implies the reduction of additive noise due to adaptive modification.

3.2 Security against Blind Steganalysis

The main drawback of the $PSSA$ [6] algorithm is that it added a substantial amount of extra additive noise during restoration process compared to the algorithms similar to the $LSBM$.

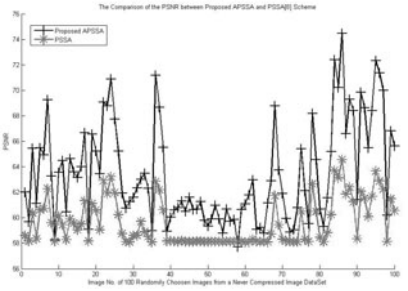


Fig. 1. Comparison of PSNR between Proposed APSSA and PSSA [6] Scheme

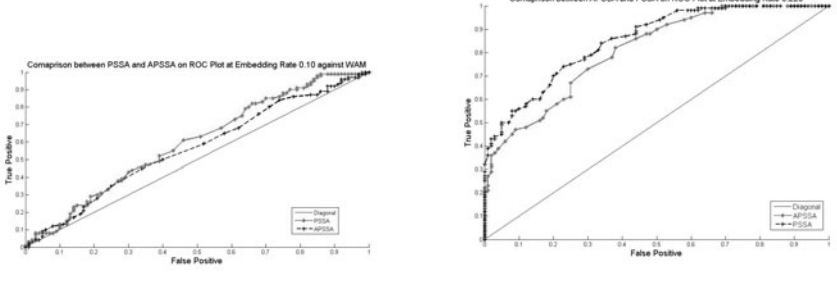
For testing the performance of the $APSSA$ algorithm, experiments are conducted on a data set of two thousand test images which were divided into two equal sets of one thousand cover images and one thousand stego images. 1000 never compressed images are taken from the UCID [4] as cover images and 1000 stego images are generated using the $APSSA$ algorithm. In these experiments, a block with four pixels is used. It is experimentally found that the payload for the bigger blocks are very less and is mostly undetectable. To evaluate the steganographic security using the proposed scheme, Area under the Receiver Operating Characteristic Curve ($AROC$) and the Detection accuracy (P_{detect}) [5] which is computed using equations 5 and 6 have been used as the evaluation metrics.

$$P_{detect} = 1 - P_{error} \tag{5}$$

$$P_{error} = \frac{1}{2} \times P_{FP} + \frac{1}{2} \times P_{FN} \tag{6}$$

where P_{FP}, P_{FN} are the probabilities of false positive and false negative respectively. A value of $P_{detect} = 0.5$ shows that the classification is as good as random guessing and $P_{detect} = 1.0$ shows a classification with 100% accuracy.

For the evaluation of the proposed $APSSA$ scheme, Wavelet absolute moment (WAM) steganalyzer [3] is considered as steganalytic attack. In Figure 2,



(a) Emb. rate 0.10 bpp (b) Emb. rate 0.225 bpp

Fig. 2. ROC plot for comparing between $APSSA$ and $PSSA$ [6] against WAM

it is shown that proposed $APSSA$ scheme is relatively less detectable than the $PSSA$ scheme [6] against WAM at the same embedding rates using never compressed image dataset as cover image source. Since, the histogram of the image is kept intact during embedding, proposed adaptive improved scheme remains undetectable against any histogram based spatial domain steganalytic attacks similar to the $PSSA$ scheme [6].

4 Conclusion

In this paper, an adaptive improvement over $PSSA$ algorithm [6] is proposed by incorporating a block based local adaptive threshold such that the amount of additive noise can be controlled adaptively using block image statistics. We have experimentally shown that the enforced adaptiveness makes the scheme more secure than its non adaptive version (PSSA) against additive noise based steganalyzers while it maintains same performance as PSSA against targeted attacks since image histogram is kept intact during embedding.

References

1. Ker, A.D.: Steganalysis of LSB matching in grayscale images. IEEE Signal processing letters 12(6), 441–444 (2005)
2. Zhang, J., Cox, I.J., Doerr, G.: Steganalysis for LSB Matching in Images with High-frequency Noise. In: Proc. IEEE 9th Workshop on Multimedia Signal Processing MMSP 2007, pp. 385–388 (2007)
3. Goljan, M., Fridrich, J., Holotyak, T.: New blind steganalysis and its implications. In: Proceedings of SPIE for Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 1–13 (2006)
4. Schaefer, G., Stich, M.: UCID - An Uncompressed Colour Image Database. In: Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia, vol. 5307, pp. 472–480 (2004)
5. Solanki, K., Sarkar, A., Manjunath, B.S.: YASS: Yet Another Steganographic Scheme That Resists Blind Steganalysis. In: Furon, T., Cayre, F., Doërr, G., Bas, P. (eds.) IH 2007. LNCS, vol. 4567, pp. 16–31. Springer, Heidelberg (2008)
6. Sur, A., Goel, P., Mukhopadhyay, J.: A Novel Steganographic Algorithm Resisting Targeted Steganalytic Attacks on LSB Matching. In: Kim, H.-J., Katzenbeisser, S., Ho, A.T.S. (eds.) IWDW 2008. LNCS, vol. 5450, pp. 199–208. Springer, Heidelberg (2009)