BASN — Learning Steganography with Binary Attention Mechanism

Yang Yang *
†‡

July 11, 2019

Abstract

Secret information sharing through image carrier has aroused much research attention in recent years with images’ growing domination on the Internet and mobile applications. However, with the booming trend of convolutional neural networks, image steganography is facing a more significant challenge from neural-network-automated tasks. To improve the security of image steganography and minimize task result distortion, models must maintain the feature maps generated by task-specific networks being irrelative to any hidden information embedded in the carrier. This paper introduces a binary attention mechanism into image steganography to help alleviate the security issue, and in the meanwhile, increase embedding payload capacity. The experimental results show that our method has the advantage of high payload capacity with little feature map distortion and still resist detection by state-of-the-art image steganalysis algorithms.

Index terms— convolutional neural network; steganography; attention mechanism

1 Introduction

Image steganography aims at delivering a modified cover image to secretly transfer hidden information inside with little awareness of the third-party
Figure 1: LSB-Matching Embedded Image Misclassification

The cover image and embedded image both use ImageNet pretrained ResNet-18 network for classification. The percentage before the predicted class label represents network’s confidence in prediction. The red, green and blue noisy images in the center represent the altered pixel locations in corresponding channels during steganography. There’re only three kinds of colors within these images where white stands for no modification, the lighter one stands for a +1 modification and the darker one stands for a -1 modification.

supervision. On the other side, steganalysis algorithms are developed to find out whether an image is embedded with hidden information or not, and therefore, resisting steganalysis detection is one of the major indicators of steganography security. In the meanwhile, with the booming trend of convolutional neural networks, a massive amount of neural-network-automated tasks are coming into industrial practices like image auto-labeling through object detection [5, 15] and classification [8, 21], face recognition [16], pedestrian re-identification [29] and etc. Images steganography is now facing a more significant challenge from these automated tasks, whose embedding distortion might influence the task result in a great manner and irresistibly lead to suspicion. Figure 1 is an example that LSB-Matching [12] steganography completely alters the image classification result from goldfish to proboscis monkey. Under such circumstances, a steganography model even with outstanding invisibility to steganalysis methods still cannot be called secure where the spurious label might re-arouse suspicion and finally, all efforts are made in vain.

1.1 Related Works

Most previous steganography models focus on resisting steganalysis algorithms or raising embedding payload capacity. BPCS [18, 19] and PVD [24]
uses adaptive embedding based on local complexity to improve embedding visual quality. HuGO [14] and S-UNIWARD [9] resist steganalysis by minimizing a suitably defined distortion function. Hu [10] adopts deep convolutional generative adversarial network to achieve steganography without embedding. Wu [26] and Baluja [1] achieve a vast payload capacity by focusing on image-into-image steganography.

1.2 Contributions of this work

In this paper, we propose a Binary Attention Steganography Network (abbreviated as BASN) architecture to achieve a relatively high payload capacity (2-3 bpp) with minimal distortion to other neural-network-automated tasks. It utilizes convolutional neural networks with two attention mechanisms, which minimizes embedding distortion to the human visual system and neural network feature maps respectively. Additionally, multiple attention fusion strategies are suggested to balance payload capacity with security, and a fine-tuning mechanism are put forward to improve the hidden information extraction accuracy.

2 Binary Attention Mechanism

Binary attention mechanism involves two attention models including image texture complexity (ITC) attention model and minimizing feature distortion (MFD) attention model. ITC model mainly focuses on deceiving the human visual system from noticing the differences out of altered pixels. MFD model minimizes the high-level features extracted between clean and embedded images so that neural networks will not give out diverge results. The attention mechanism in both models serve as a hint for steganography showing where to embed and how much information the corresponding pixel might tolerate.

The embedding and extraction overall architecture are shown in Figure 2. After two attentions are found with the binary attention mechanism, we may adopt several fusion strategies to create the final attention used for embedding and extraction.

2.1 Evaluation of Image Texture Complexity

To evaluate an image's texture complexity, variance is adapted in most approaches. However, using variance as the evaluation mechanism enforces very strong pixel dependencies. In other words, every pixel is correlated to all other pixels in the image.
We propose variance pooling evaluation mechanism to relax cross-pixel dependencies (See Equation 1). Variance pooling applies on patches but not the whole image to restrict the influence of pixel value alterations within the corresponding patches. Especially in the case of training when optimizing local textures to reduce its complexity, pixels within the current area should be most frequently changed while far distant ones are intended to be reserved for keeping the overall image contrast, brightness and visual patterns untouched.

\[
\text{VarPool2d}(X_{i,j}) = \mathbb{E}_{k_i} \left( \mathbb{E}_{k_j} \left( X_{i+k_i,j+k_j}^2 \right) \right) - \mathbb{E}_{k_i} \left( \mathbb{E}_{k_j} \left( X_{i+k_i,j+k_j}^2 \right) \right) \tag{1}
\]

\[
k_i \in \left[ -\frac{n}{2}, \frac{n}{2} \right], \quad k_j \in \left[ -\frac{n}{2}, \frac{n}{2} \right] \tag{2}
\]

In Equation 1, \( X \) is a 2-dimensional random variable which can be either an image or a feature map and \( i, j \) are the indices of each dimension. Operator \( \mathbb{E}(\cdot) \) calculates the expectation of the random variable. VarPool2d applies similar kernel mechanism as other 2-dimensional pooling or convolution operations and \( k_i, k_j \) indicates the kernel indices of each dimension.

To further show the impact of gradients updating between variance and variance pooling during backpropagation, we applied the gradients backpropagated directly to the image to visualize how gradients influences the image itself during training (See Equation 3 for training loss and Figure 3 for the impact comparison).
\[ \mathcal{L}_{\text{Variance}} = \text{Variance}(X) \] (3)
\[ \mathcal{L}_{\text{VarPool2d}} = \mathbb{E}(\text{VarPool2d}_{n=7}(X)) \] (4)

2.2 ITC Attention Model

ITC (Image Texture Complexity) attention model aims to embed information without being noticed by the human visual system, or in other words, making just noticeable difference (JND) to cover images to ensure the largest embedding payload capacity \[28\]. In texture-rich areas, it is possible to alter pixels to carry hidden information without being noticed. Finding the ITC attention means finding the positions of the image pixels and their corresponding capacity that tolerate mutations.

Here we introduce two concepts:

1. A hyper-parameter \( \theta \) representing the ideal embedding payload capacity that the input image might achieve.
2. An ideal texture-free image \( C_\theta \) corresponding to the input image that is visually similar but with the lowest texture complexity possible regarding the restriction of at most \( \theta \) changes.

With the help of these concepts, we can formulate the aim of ITC attention model as:

For each cover image \( C \), ITC model \( f_{\text{itec}} \) needs to find an attention \( A_{\text{itec}} = f_{\text{itec}}(C) \) to minimize the texture complexity evaluation function \( V_{\text{itec}} \):
The $\theta$ in Equation 6 is used as an upper bound to limit down the attention area size. If trained without it, model $f_{itc}$ is free to output all-ones matrix $A_{itc}$ to acquire an optimal texture-free image. It is well-known that an image with the least amount of texture is a solid color image, which does not help find the correct texture-rich areas.

In actual training process, the detailed model architecture is shown in Figure 6 and two parts of the equation are slightly modified to ensure better training results. First, the ideal texture-free image $C_\theta$ in Equation 5 does not indeed exist but is available through approximation nonetheless. In this paper median pooling with a kernel size of 7 is used to simulate the ideal texture-free image. It helps eliminate detailed textures within patches without touching object boundaries (See Figure 4 for comparison among different smoothing techniques). Second, we adopt soft bound limits in place of hard upper bound in forms of Equation 7 (visualized in Figure 9). Soft limits help generate smoothed gradients and provide optimizing directions.

$$\text{Area-Penalty}_{itc} = \mathbb{E}(A_{itc})^{3-2\mathbb{E}(A_{itc})}$$ (7)

The overall loss on training ITC attention model is listed in Equation 8 and Figure 5 shows the effect of ITC attention on image texture complexity.
reduction. The attention area reaches 21.2% on average, and the weighted images gain an average of 86.3% texture reduction in the validation dataset.

\[
\text{VarLoss} = \mathbb{E} \left( \text{VarPool2d} \left( A_{\text{itc}} \cdot C_{\theta} + (1 - A_{\text{itc}}) \cdot C \right) \right)
\]

\[
\text{Loss}_{\text{itc}} = \lambda \cdot \text{VarLoss} + (1 - \lambda) \cdot \text{Area} - \text{Penalty}_{\text{itc}}
\]

2.3 MFD Attention Model

MFD (Minimizing Feature Distortion) attention model aims to embed information with least impact on neural network extracted features. Its attention also indicates the position of image pixels and their corresponding capacity that tolerate mutations.

For each cover image \(C\), MFD model \(f_{\text{mfd}}\) needs to find an attention \(A_{\text{mfd}} = f_{\text{mfd}}(C)\) that minimizes the distance between cover image features \(f_{\text{nn}}(C)\) and embedded image features \(f_{\text{nn}}(S)\) after embedding information into cover image according to its attention.

\[
S = f_{\text{embed}}(C, A_{\text{mfd}})
\]

\[
\text{minimize } \mathcal{L}_{\text{mri}}(f_{\text{nn}}(C), f_{\text{nn}}(S))
\]

subject to \(\alpha \leq \frac{1}{N} \sum_{i}^{N} A_{\text{mfd}} \leq \beta\)
Here, $C$ stands for the cover image and $S$ stands for the corresponding embedded image. $\mathcal{L}_{fmrl}(\cdot)$ is the feature map reconstruction loss and $\alpha, \beta$ are thresholds limiting the area of attention map acting the same role as $\theta$ in the ITC attention model.

The actual ways of training the MFD attention model is split into 2 phases (See Figure 6). The first training phase aims to initialize the weights of encoder blocks using the left path shown in Figure 6 as an autoencoder. In the second training phase, all the weights of decoder blocks are reset and takes the right path to generate MFD attentions. The encoder and decoder block architectures are shown in Figure 7.

The weights of two MFD blocks colored in purple are shared while the weights of two task specific neural network blocks colored in yellow are frozen. In the training process, task specific neural network works only as a feature extractor and therefore it can be simply extended to multiple tasks by reshaping and concatenating feature maps together. Here we adopt ResNet-18 [8] as an example for minimizing embedding distortion to the classification task.

The overall training pipeline in the second phase is shown in Figure 8. The overall loss on training MFD attention model (phase 2) is listed in Equation 13. The $\mathcal{L}_{fmrl}$ (Feature Map Reconstruction Loss) uses $L_2$ loss to reconstruct between cover image extracted feature maps and embedded ones. The $\mathcal{L}_{cerl}$ (Cover Embedded image Reconstruction Loss) and $\mathcal{L}_{atrl}$ (Attention Reconstruction Loss) uses $L_1$ loss to reconstruct between the cover images and the embedded images and their corresponding attentions. The $\mathcal{L}_{atap}$ (AT-
Figure 7: MFD Attention Mechanism Training Pipeline

Figure 8: The Encoder and Decoder Block of the MFD Attention Model
Attention Area Penalty) also applies soft bound limit in forms of Equation 14 (visualized in Figure 9). The visual effect of MFD attention embedding with random noise is shown in Figure 10.

\[
\text{Loss}_{\text{mfd}} = \mathcal{L}_{\text{fmrl}} + \mathcal{L}_{\text{cerl}} + \mathcal{L}_{\text{atrl}} + \mathcal{L}_{\text{atap}}
\]

(13)

\[
\text{Area-Penalty}_{\text{mfd}} = \frac{1}{2} \cdot (1.1 \cdot \mathbb{E}(A_{\text{mfd}}))^8 \cdot \mathbb{E}(A_{\text{mfd}})^{-0.1}
\]

(14)
3 Fusion Strategies, Finetune Process and Inference Techniques

The fusion strategies help merge ITC and MFD attention models into one attention model, and thus they are substantial to be consistent and stable. In this paper, two fusion strategies being minima fusion and mean fusion are put forth as Equation 15 and 16. Minima fusion strategy aims to improve security while mean fusion strategy generates more payload capacity for embedding.

\[ A_f = \min(A_{\text{itc}}, A_{\text{mfd}}) \]  
\[ A_f = \frac{1}{2}(A_{\text{itc}}, A_{\text{mfd}}) \]

After a fusion strategy is applied, finetuning process is required to improve attention reconstruction on embedded images. The finetune process is split into two phases. In the first phase, the ITC model is finetuned as Figure 11. The two ITC model colored in purple shares the same network weights and the MFD model weights are freezed. Besides from the image texture complexity loss (Equation 8) and the ITC area penalty (Equation 7), the loss additionally involves an attention reconstruction loss using \( L_1 \) loss similar to \( L_{\text{atr}} \) in Equation 13. In the second phase, the new ITC model is freezed, and the MFD model is finetuned using its original loss (Equation 13).

The ITC model, after finetune, appears to be more interested in the texture-complex areas while ignores the areas that might introduce noises into the attention (See Figure 12).

When using the model for inference after finetuning, two extra techniques are proposed to strengthen steganography security. The first technique is
The first column shows the original image, the second column shows the ITC attention before any finetune, the third column shows the ITC attention after finetuning for minima fusion strategy, and the forth column shows the ITC attention after finetuning for mean fusion strategy.

named \textit{Least Significant Masking (LSM)} which masks the lowest several bits of the attention during embedding. After the hidden information is embedded, the masked bits are restored to the original data to disturb the steganalysis methods. The second technique is called \textit{Permutative Straddling}, which sacrifices some payload capacity to straddle between hidden bits and cover bits \cite{23}. It is achieved by scattering the effective payload bit locations across the overall embedded locations using a random seed. The overall hidden bits are further re-arranged sequentially in the effective payload bit locations. The random seed is required to restore the hidden data.

\section{Experiments}

\subsection{Experiments Configurations}
To demonstrate the effectiveness of our model, we conducted experiments on ImageNet dataset \cite{3}. Specially, ILSVRC2012 dataset with 1,281,167 images is used for training and 50,000 for testing. Our work is trained on one NVidia GTX1080 GPU and we adopt a batch size of 32 for all models. Optimizers and learning rate setup for ITC model, MFD model 1\textsuperscript{st} phase and MFD model 2\textsuperscript{nd} phase are Adam optimizer \cite{11} with 0.01, Nesterov momentum optimizer \cite{20} with 1e-5 and Adam optimizer with 0.01 respectively.
| Model                | BSER (%) | Payload (bpp) |
|----------------------|----------|---------------|
| Min-LSM-1            | 1.06%    | 1.29          |
| Min-LSM-2            | 0.67%    | 0.42          |
| Mean-LSM-1           | 2.22%    | 3.89          |
| Mean-LSM-2           | 3.14%    | 2.21          |
| Min-LSM-1-PS-0.6     | 0.74%    | 0.80          |
| Min-LSM-1-PS-0.8     | 0.66%    | 0.80          |
| Mean-LSM-1-PS-1.2    | 0.82%    | 1.20          |
| Mean-LSM-2-PS-1.2    | 0.93%    | 1.20          |

Table 1: Different Embedding Strategies Comparison

In the model name part, the value after LSM is the number of bits masked during embedding process and the value after PS is the maximum payload capacity the embedded image is limited to during permutative straddling.

All the validation processes use the compressed version of *The Complete Works of William Shakespeare* [17] provided by Project Gutenberg [7]. It is downloaded here at [8].

The error rate uses BSER (Bit Steganography Error Rate) shown in Equation 17.

\[
\text{BSER} = \frac{\text{Number of redundant bits or missing bits}}{\text{Number of hidden information bits}} \times 100\% \quad (17)
\]

4.2 Different Embedding Strategies Comparison

Table 1 presents a performance comparison among different fusion strategies and different inference techniques. These techniques offer several ways to trade off between error rate and payload capacity. With *Permutative Straddling*, it is further possible to precisely handle the payload capacity during transmission.

4.3 Steganalysis Experiments

To ensure that our model is robust to steganalysis methods, we test our models using StegExpose [2] with linear interpolation of detection threshold from 0.00 to 1.00 with 0.01 as the step interval. The ROC curve is shown in Figure 14 where true positive stands for an embedded image correctly identified that there are hidden data inside while false positive means that a clean figure is falsely classified as an embedded image. The figure shows
a comparison among our several models, StegNet [26] and Baluja-2017 [1] plotted in dash-line-connected scatter data. It demonstrates that StegExpose can only work a little better than random guessing and most BASN models perform better than StegNet and Baluja-2017.

Our model is also further examined with learning-based steganalysis methods [13, 4, 27]. All of these models are trained with our cover and embedded images. Their corresponding ROC curves are shown in Figure 14. SRM [4] method works quite well on our model with a larger payload capacity, however in real-world applications we can always keep our dataset private and thus ensuring high security in resisting detection from learning-based steganalysis methods.

4.4 Feature Distortion Analysis

Figure 15 shows that our model has very little influence on targeted neural-network-automated tasks, which in this case is classification. Most embedded images, even carrying with more than 3 bpp of hidden information, takes an average of only 2% distortion.

5 Conclusion

This paper proposes an image steganography method based on a binary attention mechanism to ensure little influence steganography is made to neural-network-automated tasks. The first attention mechanism, image texture complexity (ITC) model, help track down the pixel locations and their tol-
Figure 14: ROC Curves: Steganalysis with StegExpose, SPAM Features, SRM Features and Yedroudj-Net
The second mechanism, minimizing feature distortion (MFD) model, further keeps down the embedding impact through feature map reconstruction. Moreover, some attention fusion and finetune techniques are also proposed in this paper to improve security and hidden information extraction accuracy. The imperceptibility of secret information by our method is proved such that the embedding images can effectively resist detection by several steganalysis algorithms.

References

[1] Shumeet Baluja. Hiding images in plain sight: Deep steganography. In *Advances in Neural Information Processing Systems*, pages 2069–2079, 2017.

[2] Benedikt Boehm. StegExpose - A Tool for Detecting LSB Steganography. *arXiv e-prints*, 2014. arXiv: 1410.6656.

[3] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei. ImageNet: A Large-Scale Hierarchical Image Database. 2009.
[4] Jessica Fridrich and Jan Kodovsky. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, 7(3):868–882, 2012.

[5] Ross Girshick. Fast r-cnn. In *Proceedings of the IEEE international conference on computer vision*, pages 1440–1448, 2015.

[6] Project Gutenberg. The complete works of william shakespeare by william shakespeare - free ebook., 2018. [Online; Accessed 13-Nov-2018].

[7] Project Gutenberg. Project gutenberg, 2018. [Online; Accessed 13-Nov-2018].

[8] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.

[9] Vojtěch Holub, Jessica Fridrich, and Tomáš Denemark. Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*, 2014(1):1, 2014.

[10] Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, and Bin Li. A novel image steganography method via deep convolutional generative adversarial networks. *IEEE Access*, 6:38303–38314, 2018.

[11] Diederik Kingma and Jimmy Ba. Adam: A Method for Stochastic Optimization. *arXiv e-prints*, 2014. arXiv:1412.6980.

[12] J. Mielikainen. Lsb matching revisited. *IEEE signal processing letters*, 13(5):285–287, 2006.

[13] Tomáš Pevný, Patrick Bas, and Jessica Fridrich. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on information Forensics and Security*, 5(2):215–224, 2010.

[14] Tomáš Pevný, Tomáš Filler, and Patrick Bas. Using high-dimensional image models to perform highly undetectable steganography. In *International Workshop on Information Hiding*, pages 161–177. Springer, 2010.

[15] Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi. You only look once: Unified, real-time object detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 779–788, 2016.
[16] Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 815–823, 2015.

[17] W. Shakespeare. The Complete Works of William Shakespeare. 1994.

[18] Jeremiah Spaulding, Hideki Noda, Mahdad N Shirazi, and Eiji Kawaguchi. Bpcs steganography using ezw lossy compressed images. Pattern Recognition Letters, 23(13):1579–1587, 2002.

[19] Shuliang Sun. A new information hiding method based on improved bpcs steganography. Advances in Multimedia, 2015:5, 2015.

[20] Ilya Sutskever, James Martens, George Dahl, and Geoffrey Hinton. On the importance of initialization and momentum in deep learning. In International conference on machine learning, pages 1139–1147, 2013.

[21] Christian Szegedy, Sergey Ioffe, Vincent Vanhoucke, and Alexander A Alemi. Inception-v4, inception-resnet and the impact of residual connections on learning. In Thirty-First AAAI Conference on Artificial Intelligence, 2017.

[22] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, and Min-Shiang Hwang. A high quality steganographic method with pixel-value differencing and modulus function. Journal of Systems and Software, 81(1):150–158, 2008.

[23] Andreas Westfeld. F5—a steganographic algorithm. In Ira S. Moskowitz, editor, Information Hiding, pages 289–302, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[24] Da-Chun Wu and Wen-Hsiang Tsai. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9-10):1613–1626, 2003.

[25] H-C Wu, N-I Wu, C-S Tsai, and M-S Hwang. Image steganographic scheme based on pixel-value differencing and lsb replacement methods. IEEE Proceedings-Vision, Image and Signal Processing, 152(5):611–615, 2005.

[26] Pin Wu, Yang Yang, and Xiaoqiang Li. Image-into-image steganography using deep convolutional network. In Richang Hong, Wen-Huang Cheng, Toshihiko Yamasaki, Meng Wang, and Chong-Wah Ngo, editors,
Advances in Multimedia Information Processing – PCM 2018, pages 792–802, Cham, 2018. Springer International Publishing.

[27] Mehdi Yedroudj, Frédéric Comby, and Marc Chaumont. Yedroudj-net: An efficient cnn for spatial steganalysis. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 2092–2096. IEEE, 2018.

[28] Xiaohui Zhang, Weisi Lin, and Ping Xue. Just-noticeable difference estimation with pixels in images. Journal of Visual Communication and Image Representation, 19(1):30–41, 1 2008.

[29] Zhun Zhong, Liang Zheng, Zhedong Zheng, Shaozi Li, and Yi Yang. Camera style adaptation for person re-identification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 5157–5166, 2018.