DeepKeyStego: Protecting Communication by Key-dependent Steganography with Deep Networks

Zheng Li[1], Ge Han[1], Chengyu Hu[2] and Shanqing Guo*[2]
[1]School of Computer Science and Technology, Shandong University
[2]School of Cyber Science and Technology, Shandong University

01 Motivation

- **Goal**: protect privacy-sensitive communication against eavesdropping over public communication channels

- Tranditional steganographic schemes are cool, but
  - designed with prescribed human based rules
  - effectively detected by existing steganalysis tools

- Deep Neural Networks are applied to increasingly complex tasks,
  - end-to-end objectives that go beyond simple functional specifications
  - without being taught specific algorithms for these purposes.

02 Related Works

- Classical Methods:
  - the Least Significant Bit (LSB) algorithm
  - WOW, HUGO, S-UNIWARD

- DNN-based Methods:
  - steganographic generative adversarial network (SGAN)
  - ste-GAN-ography

03 Framework overview

- Two settings: symmetric and asymmetric
- Four models: Alice, Bob, Eve, and pK Generator

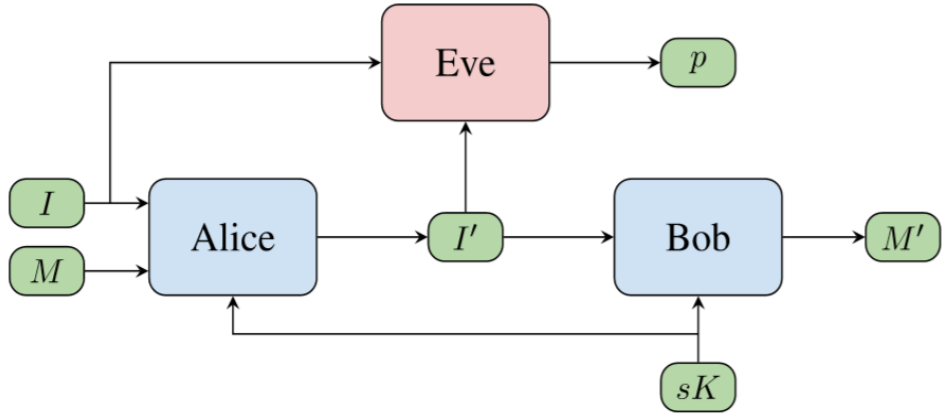


Fig. 1. Symmetric steganography

- Model **Alice**: an encoder that can hide the secret message into a cover image.
- Model **Bob**: a decoder that can recover the secret message from stego image with the aid of key
- Model **Eve**: a discriminative adversary that attempts to distinguish stego images from real ones
- Model **pK Generator**: a public-key generator

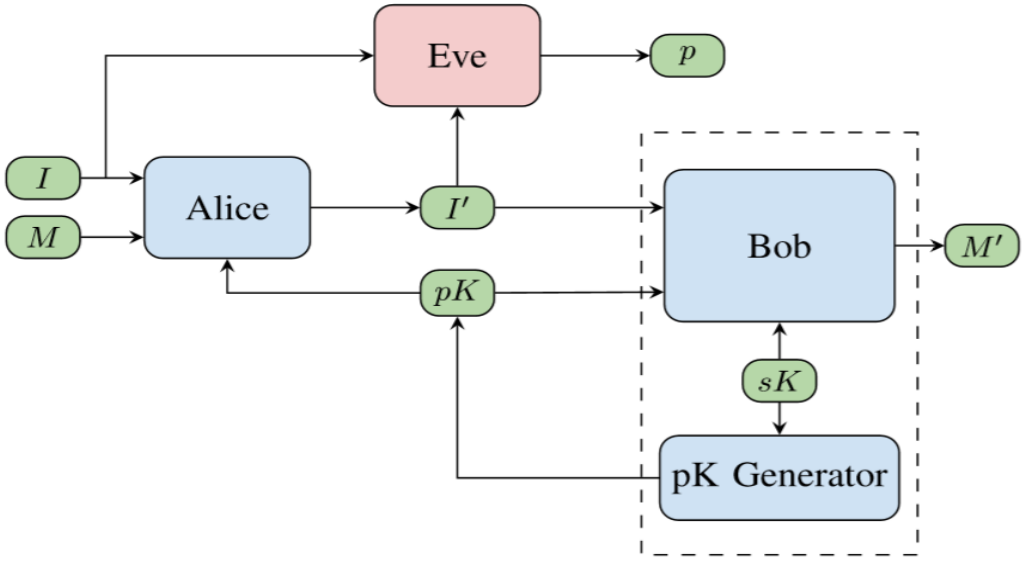


Fig. 2. Asymmetric steganography

04 Asymmetric workflow

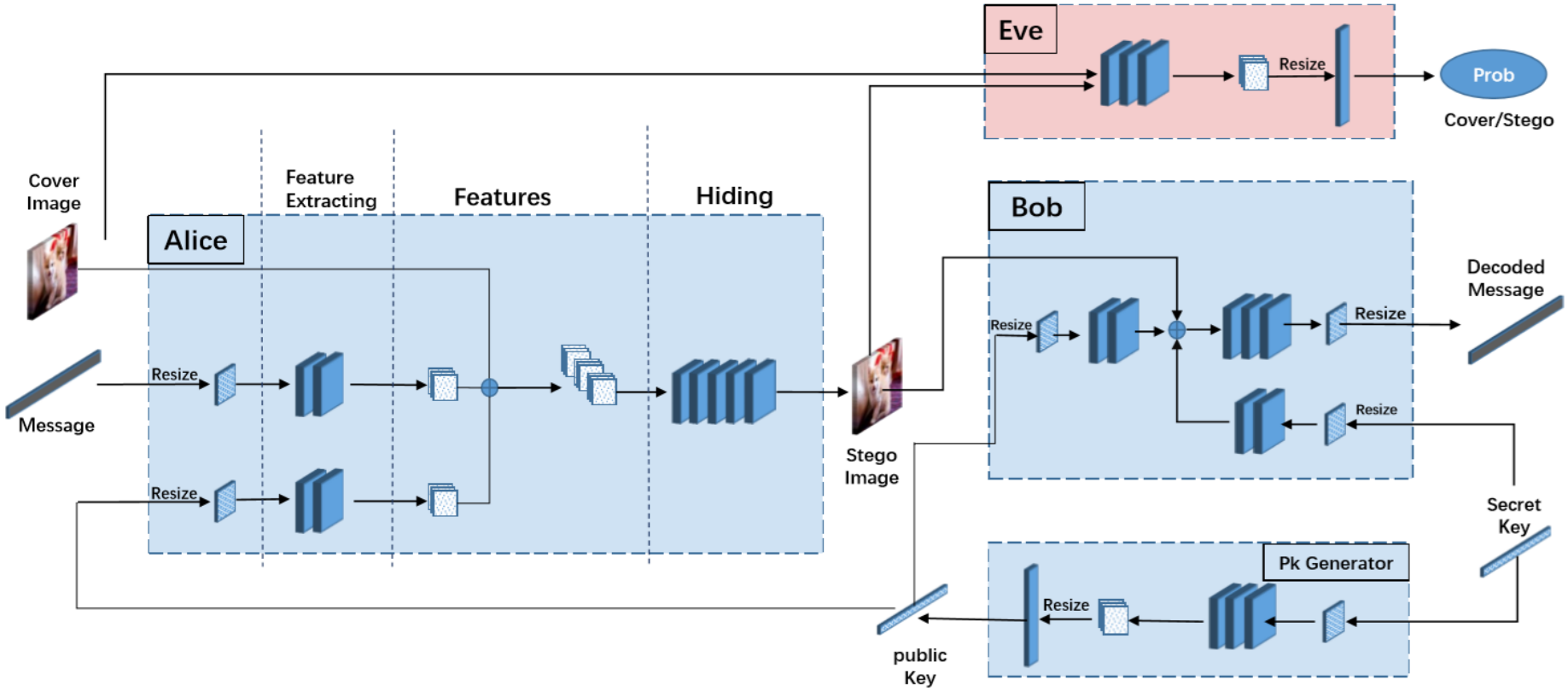


Fig. 3. The asymmetric workflow of DeepKeyStego

05 Loss Function

Eve: $p(\tilde{I}) = \begin{cases} 1, & \tilde{I} = I \\ 0, & \tilde{I} = I' \end{cases}$

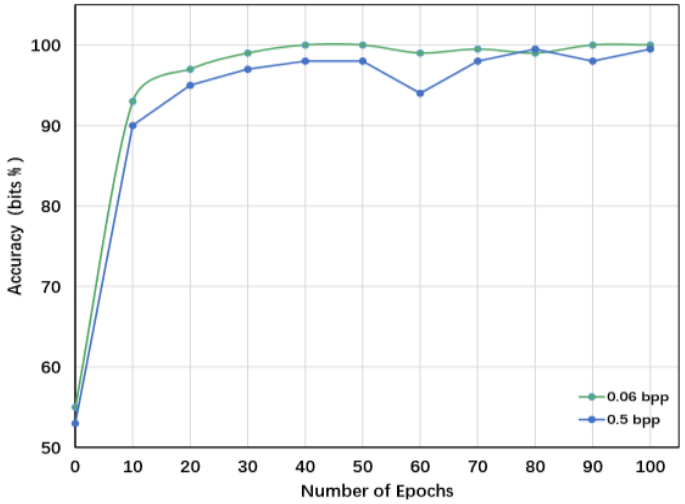
$$argmin_{\theta_E} \log\big(1 - p(\mathrm{I})\big) + \log(p(I'))$$

Alice, Bob and pk Generator:

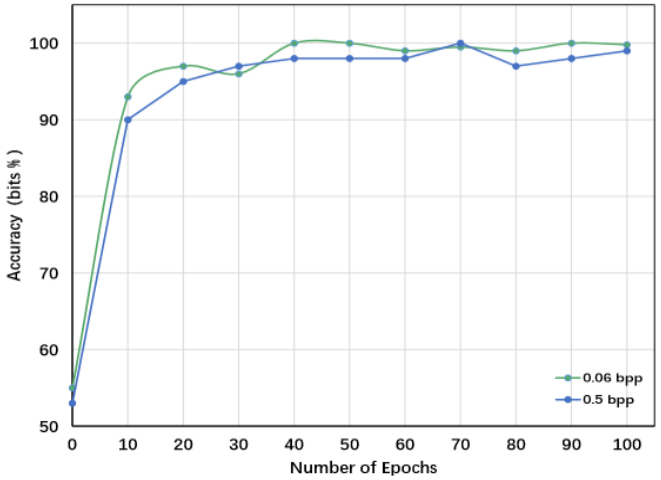
$$argmin_{\theta_A \theta_B \theta_{\mathrm{p}K}} \alpha MSE(I, I') + \beta SSIM(I, I') + \gamma L_1(M, M') + \delta \log(1 - p(I'))$$

06 Implementation

- Dataset:
  - ImageNet
  - Training Set: **80000**, Testing Set: **10000**
  - ImageSize: **128 * 128 *3**
  - Key Length: **1024bits**
  - Message Length: **1024bits** or **8192 bits**
    - **o.o6bpp** or **0.5bpp** (the number of bits per pixel)



(a) Bob decoding success for symmetric

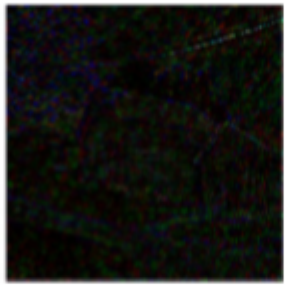
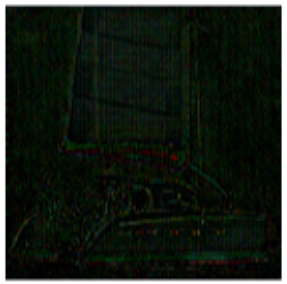
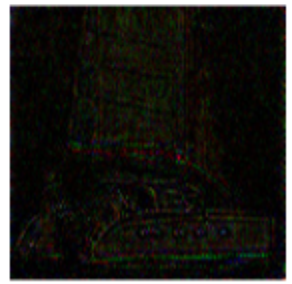


(b) Bob decoding success for asymmetric

07 Evaluation

invisibility, the alteration made to cover images

Visual effects of resultant steganographic encoders.

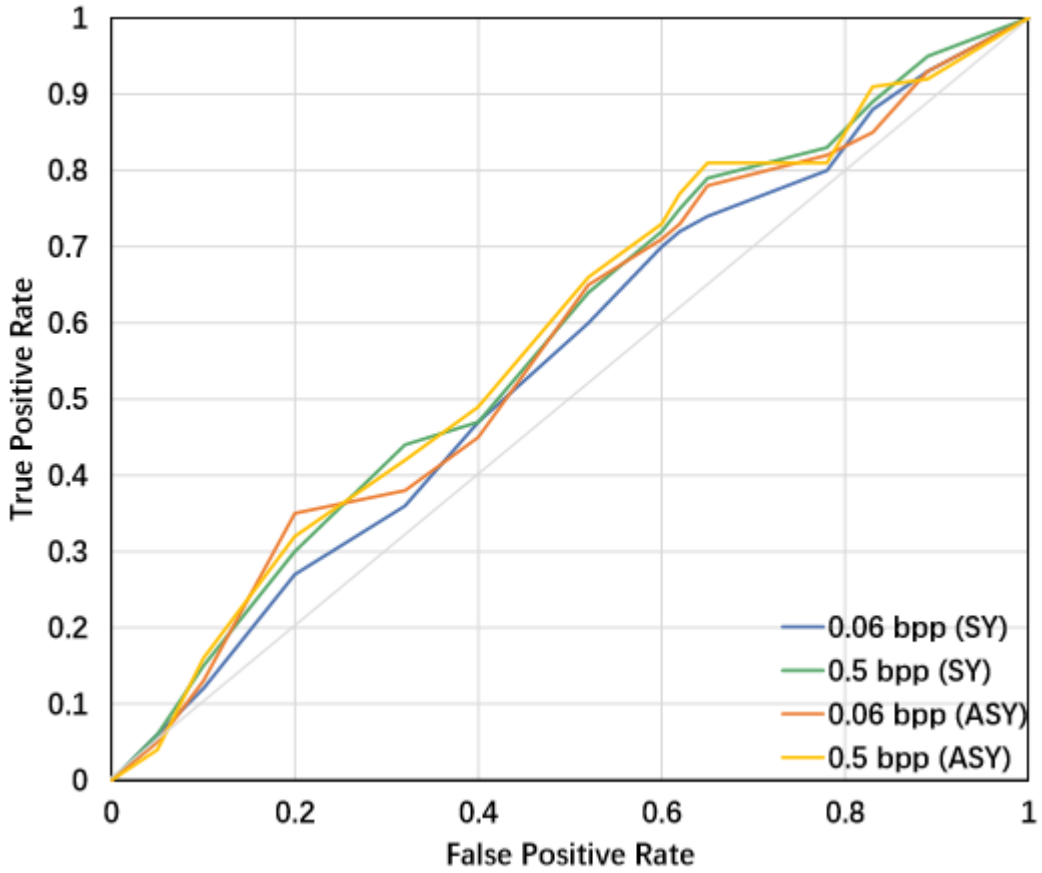
Cover	Symmetric(stego / difference×1 / difference×5)			Asymmetric(stego / difference×1 / difference×5)		
						
						

08 Evaluation

undetectability, the stego images can evade steganalysis detections

Accuracy of distinguishing between cover and stego images for the steganalyzers ATS

Method	Bits per pixel	Detection Rate (ATS) (%)
WOW	0.5	75%
HUGO	0.5	85%
S-UNIWARD	0.5	83%
DeepKeyStego (symmetric)	0.5	**51%**
DeepKeyStego (asymmetric)	0.5	**50%**



09 Evaluation

unrecoverability, the degree to which attackers can recover the content of secret messages

integrity, the performance of the decoder in a practical situation

An example in simulated communication

Secret Message	Before encode	Key	After decode	Decoded Message
Two months ago, across an assembly-room table in a factory in Jacksonville, Fla., President Barack Obama was talking to me about...	01010100 01110111 ... 01110100 01100001 ... 01110101 01110100	Correct	01010100 01110111 ... 01110100 01100011 ... 01110001 01110100	Two months ago, across an assembly-room tcble in a factory in Jacksonville, Fla., President Barack Obama was talking to me aboqt...
		Wrong	10111111 10101111 ... 11010100 10101001 ... 00111010 11100101	¿¯°Úÿ¿òNpu¶QÖ • [9³ gýUr×å[õ˜m³ ÒTµÖf [¦ ÝV=û¼\vÑÔ© • } ÎÊkÕå4W/ Ë3*ÕæëvGoÎZ½R®É&Ö³ Ý- ÖdÃQþU>sW$˜Bc?ò8ò©Ý¢áÖ³ _ • Û:å

10 Conclusion

- Symmetric (secret-key) and Asymmetric (public-key) steganographic scheme are separately proposed
- DeepKeyStego achieved excellent invisibility and outstanding undetectability better than previous methods.
- taking advantage of keys to enhance the security of steganography against any adversary .
- our scheme is effective and practical for information hiding in communication.

Thanks!