International Journal of Digital Crime and Forensics
Volume 13 • Issue 4 • July-August 2021

Coverless Information Hiding Based on WGAN-GP Model

Xintao Duan, Henan Normal University, Xinxiang, China
Baoxia Li, Henan Normal University, Xinxiang, China
Daidou Guo, Henan Normal University, Xinxiang, China
Kai Jia, Henan Normal University, Xinxiang, China
En Zhang, Henan Normal University, Xinxiang, China
Chuan Qin, University of Shanghai for Science and Technology, Shanghai, China

ABSTRACT

Steganalysis technology judges whether there is secret information in the carrier by monitoring the abnormality of the carrier data, so the traditional information hiding technology has reached the bottleneck. Therefore, this paper proposed the coverless information hiding based on the improved training of Wasserstein GANs (WGAN-GP) model. The sender trains the WGAN-GP with a natural image and a secret image. The generated image and secret image are visually identical, and the parameters of generator are saved to form the codebook. The sender uploads the natural image (disguise image) to the cloud disk. The receiver downloads the camouflage image from the cloud disk and obtains the corresponding generator parameter in the codebook and inputs it to the generator. The generator outputs the same image for the secret image, which realized the same results as sending the secret image. The experimental results indicate that the scheme produces high image quality and good security.

KEYWORDS

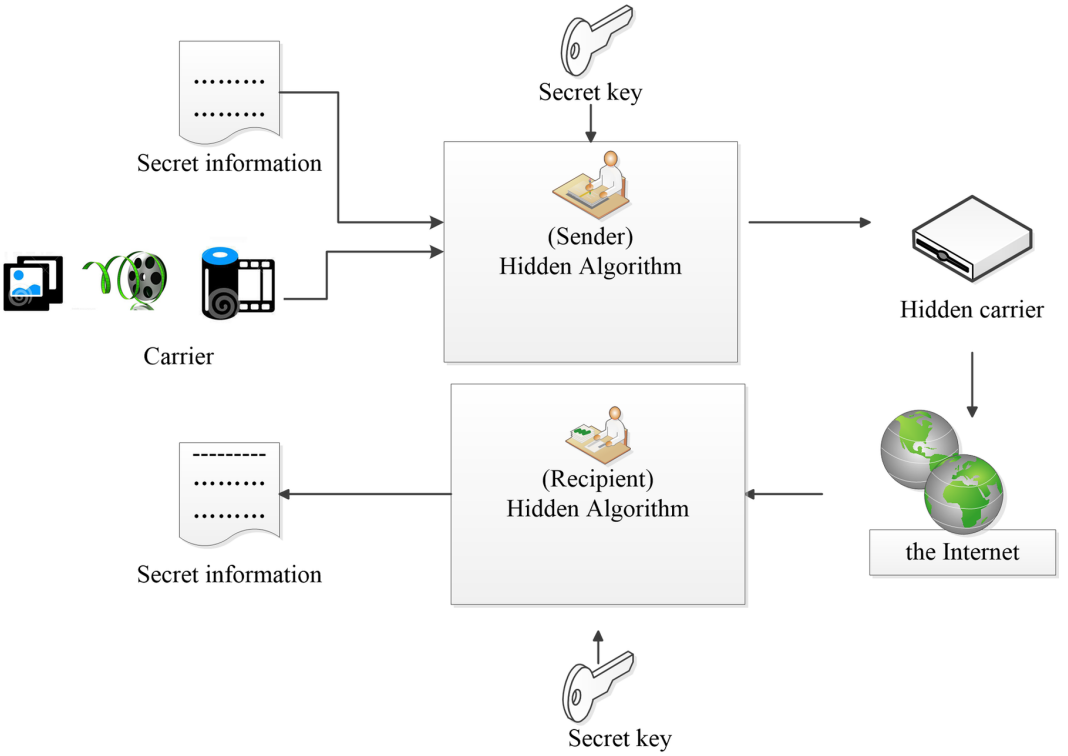
Coverless Information Hiding, Generative Adversarial Network, WGAN-GP

INTRODUCTION

Network communication and information technology have developed rapidly in the era of increasing net-workization. Cloud computing has provided enough space for individuals and enterprised to store multimedia data(Khan et al., 2018). Users can use the cloud to store and share data. There are two ways to prevent image information from leaking: encryption and information hiding (Guo et al., 2011). Encryption technology of image is to ensure the security of images, which uses digital image matrix features to change pixels according to the transformation rules of images in space or transform domain to achieve encrypted values (Liu et al., 2013; Wang et al., 2005; Samidha & Agrawal, 2013; Hemalatha et al., 2013). However, it will cause image distortion and make the image into a form of noise or texture, which may cause suspicion of the attacker and increase the possibility of information leakage, loss and tampering (Dang & Chau, 2000). The significant information was embed into the carrier by modifying the carrier data (e.g. digital image, video, audio, etc.) to realize the hiding of the important information. The procedure of information hiding avoids the attention of attackers (Sakkara & Somashekar, 2012; Zhou & Chen, 2006; Zhang et al., 2003). Moreover, digital image

DOI: 10.4018/IJDCF.20210701.oa5

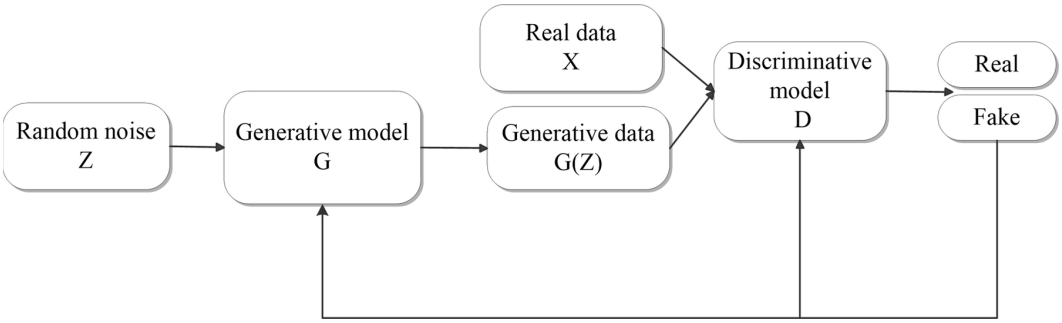
Figure 1. Typical model of information hiding



contains a number of information, and it is the most widely used as an ideal information hiding carrier and it is the most widely used as an ideal information hiding carrier (Liang&Wang, 2007; Qian&Xu, 2018; Qian & Zhang, 2016; Wang & Zhang, 2002; Ren&Sui, 2002). Technology of the classical image information hiding constitutes of spatial domain information hiding and transforms domain information hiding. The methods of the spatial domain information hiding include Least Significant Bit (LSB)(Chan & Cheng, 2004), Adaptive Least Significant Bit (Yang&Weng, 2008), Pixels Value Differencing (PVD)(Wu&Tsai, 2003), S-UNIWARD(Holub&Fridrich, 2014), and WOW (Holub & Fridrich, 2012) etc. The methods of the transform domain include Discrete Fourier Transform (Chaumont & Puech, 2006), Discrete Cosine Transform (Cox&Kilian, 1996), and Discrete Wavelet Transform (Lin&Horng, 2008) information hiding and so on. All of these methods embed secret information according to certain rules through modifying the vector, and consequentially leave modified marks on the vector. Therefore, the information hiding methods mentioned above are difficult to resist detection of various steganalysis methods. The principles of typical information hiding have been shown in Figure 1.

Objective to effectively resist the test of steganalysis methods, Zhou et al. used the new conception of coverless information hiding, and compared with the classic information hiding method, the coverless information hiding doesn't need to encode the significant information into the carrier (Zhou&Cao, 2016). In (Zhou&Cao, 2016), the bag-of-words model is used to extract the visual keywords of the image. To indicate information that needs to be hidden, this realizes the hiding of the text information in the image. The method wouldn't the modify the carrier. However, a large number of codebook needs to be built, which has large storage overhead and small hiding capacity. In (Zhang&Qian, 2016), the structural information hiding is proposed, but the object library that synthesizes the dense carrier needs to be segmented from a large number of normal image libraries,

Figure 2. Structure of GAN



so the method is inefficient. This paper proposed coverless information hiding based on WGAN-GP model. The scheme doesn't change cover image and can be effectively prevented from being detected by the steganography analysis tool. The work mainly includes the following points.

1. The WGAN-GP network was built and trained with disguise and secret images. As the model was stabilized, the parameters of generator were saved to build the parameters of generator codebook.
2. The generator is only available on both sides. The camouflage image uploaded by the sender doesn't contain any information of the secret image. Even if the attacker finds the disguise image, but does not know the generator network structure, the secret image can't be cracked.
3. First, the receiver downloads the disguise image, then obtains the corresponding parameters of generator from the codebook, and then sends them to the generator to generate an image The method doesn't modify the secret image, which enhances the security of communication.

RELATED WORKS

Generative Adversarial Network (GAN)

A GAN mainly consists of two unaided networks: the generative network (G) and the discriminative network (D). The G is just like the counterfeiting team, and the D is just like the police trying to detect counterfeit money. The two sides change their methods to each other until the counterfeit cannot be distinguished from the real one (Goodfellow et al., 2014). The structure of GAN is displayed in Figure 2:

In Figure 2 G gets a stochastic noise and outputs a picture through the noise, represented as $G(z)$, and D determines whether a picture is a true picture. Its input is true data, and then its output is 1, which means it is a real picture. If the input is a pseudo sample such as $G(z)$, the output is 0, which means the input is a fake picture.

In the training process, the G and the D are continuously optimized, and the purpose of G is to generate a more realistic image to deceive D as much as possible. The target of D is which image is generated by G, and which one is a real image. The above process can be expressed as the following formula (1): The loss function formula of G of WGAN is (1) formula:

$$\min_{G}\max_{D} V(D,G) = E_{x\sim p_{data}(x)}[\log D(x)] + E_{z\sim P_z(z)}[\log(1-\log D(G(z)))]. \quad (1)$$

The fixed G optimizes D, and the function of the D is formula (2):

$$\max_{D} V(D,G) = E_{x\sim p_{data}(x)} E[\log(D(x))] + E_{x\sim p_z(z)}[\log(1-D(G(z)))] \tag{2}$$

The fixed D optimizes the G, and the G loss function is the formula (3):

$$\min_{G} V(D,G) = E_{x\sim p_z(z)}[\log(1-D(G(z)))] \tag{3}$$

The true data was expressed by x, the noise of the input G was expressed by Z, and $G(Z)$ is the data generated by the G. $p_z(z)$ was the noise variable distribution. $D(x)$ was the probability that the D judges whether the data is real. When the G is fixedly generated, the optimization of the D can be understood as follows: the input is from the real data, the D optimizes the network structure to output 1 itself, the input comes from the generated data, and the D optimizes the network structure to output 0; When the D is fixed, G optimizes its own network to output its own samples as much as possible with real data, and after the generated samples pass the discrimination of D, D outputs a high probability. However, the GAN has problems such as unstable model and difficult training. WGAN is an improvement after GAN. The main improvement is that the last layer of the D removes the sigmoid. The loss of the G and the D does not take the log . WGAN solves the phenomenon of instability GAN training and network collapse (Arjovsky et al., 2017).

The loss function of the D of WGAN is as following:

$$-E_{x\sim p_g}[f_w(x)] - E_{x\sim p_r}[f_w(x)] \tag{4}$$

The loss function formula of G of WGAN is as follows:

$$-E_{x\sim p_g}[fw(x)] \tag{5}$$

p_g is the distribution of generators on dataset x. Up to now, the network structure of WGAN is still widely used, but there are still problems of training difficulties and slow convergence speed in the actual experiment process of WGAN, which are not obvious compared with traditional GAN (Zhou et al., 2016).

Improved Training of Wasserstein GANs (WGAN-GP)

WGAN fails to limit D to 1-lipschitz function, which is equivalent to the expression (6):

$$D \in 1-Lipschitz \Leftrightarrow \| \nabla_x D(x) \| \leq 1 \ for\ all\ x \tag{6}$$

For a differentiable function, the differential function is a 1-Lipschitz function if and only if the modulus of the gradient is less than or equal to 1 for any x . Add a condition to the target expression of discriminator, and the target expression of D is (7):

$$V(G,D) \approx \max_{D} \{E_{x\sim p_{data}}[D(x)] - E_{x\sim p_G}[D(x)] - \lambda \int_x \max(0, \| \nabla_x D(x) \| - 1) dx\} \tag{7}$$

The added condition is that the modulo of all gradients does not satisfy the item less than or equal to 1, assigns a penalty parameter to these items, calculates the penalty value and accumulating all the penalty values. When the accumulated penalty is large enough, it will the dragged value eventually leads to such a D is no longer the most solvable.

$$V(G,D) \approx \max_{D}\{E_{x\sim p_{data}}[D(x)] - E_{x\sim p_G}[D(x)] - \lambda E_{x\sim p_{penalty}}[\max(0,\| \nabla_x D(x) \| -1)]\} \tag{8}$$

The purpose of the entire WGAN is to gradually move closer and the area between and between must have a substantial impact on the discriminator. Therefore, the range of x in the penalty term is reduced to $p_{penalty}$, which is the region between p_G and p_{data} , and the target expression is converted from (7) to (8).

$$V(G,D) \approx \max_{D}\{E_{x\sim p_{data}}[D(x)] - E_{x\sim p_G}[D(x)] - \lambda Ex \sim p_{x\sim penalty}[(\| \nabla_x D(x) \| -1)^2]\} \tag{9}$$

The closer the penalty is to 1, the faster the training, the less the penalty, the better the effect. The expression can be written as (9) (Gulrajani et al., 2017).

PROPOSED METHOD

Inspired by inputting WGAN-GP random noise to generate handwritten fonts, one image is used instead of random noise to generate another image. In this article, the camouflage image that has nothing to do with the secret image to the generator. G generates a visually identical image to a secret image. In the paper first put forward the coverless information hiding based on WGAN-GP model. The content includes the following parts.

Codebook Database

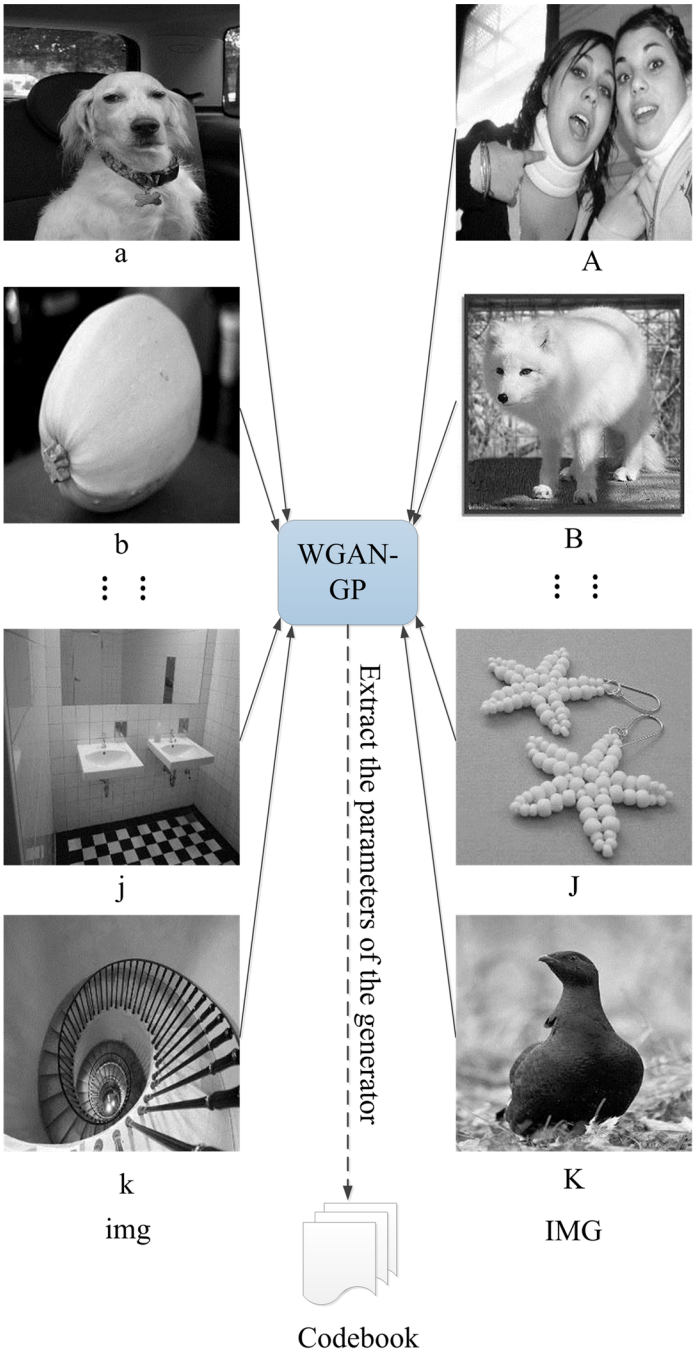
The camouflage image (img) and the secret image (IMG) were transmited to the G and D of the WGAN-GP model respectively. After the model is trained to be stable, the G's parameters of the IMG image generated by the img image through the G are saved. In this experiment, 100,000 images were extracted from the ImageNet (Deng et al., 2009) dataset (the color images were changed to grayscale images and the size of these iamges were changed to 256×256), and the IMG image and img image were 50,000. Or say, the codebook constructs of G's parameters that generate 50,000 IMG' images from 50,000 img images. The process of creating the codebook is shown in Figure 3.

Our WGAN-GP model

The WGAN-GP model is build, and the network parameters of G are initialized. At first, we construct the WGAN-GP model, then initialize the model parameters, and finally train the model with the img image and the IMG image. The sender inputs the img image and the IMG image into the WGAN-GP for training, and retains the parameters of G after the model is stable. The process of sender hiding is shown in Figure 4.

Firstly, the receiver downloads the img image from the cloud disk, and then obtains the parameters of the corresponding G from the codebook, and transmits the img image and the parameters of G to the G to generate an IMG' image. And the process of the receiver reveals the IMG' image is shown in Figure 5.

Figure 3. Create the codebook



The Process of Experiment

The dispatcher and the receiptor agree in advance to use the same G (only the sender and the receiver have). The sender trains the WGAN-GP with img images and IMG images, and the parameters of G and img images are uploaded to the cloud disk after the model training is stabilized. First, the receiver

Figure 4. The WGAN-GP model proposed in the paper

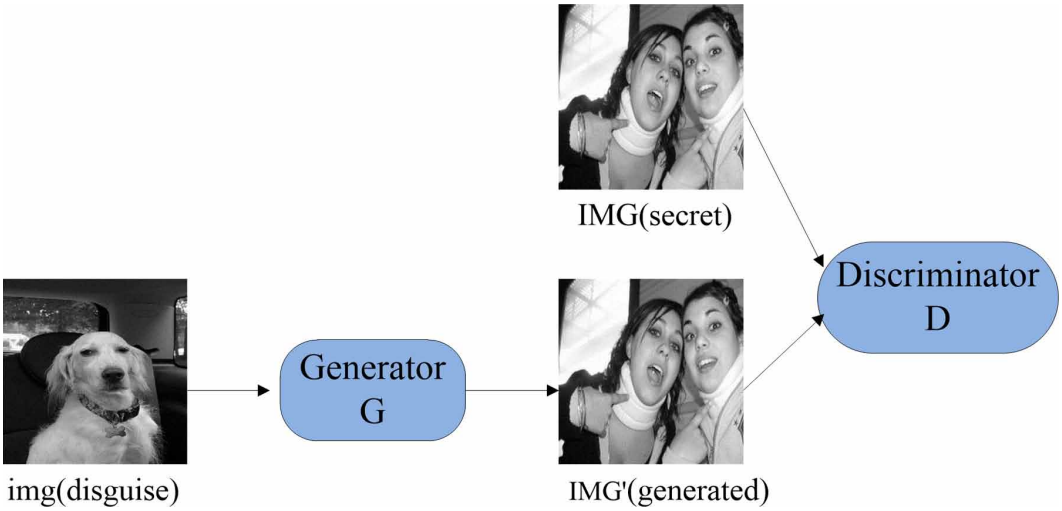
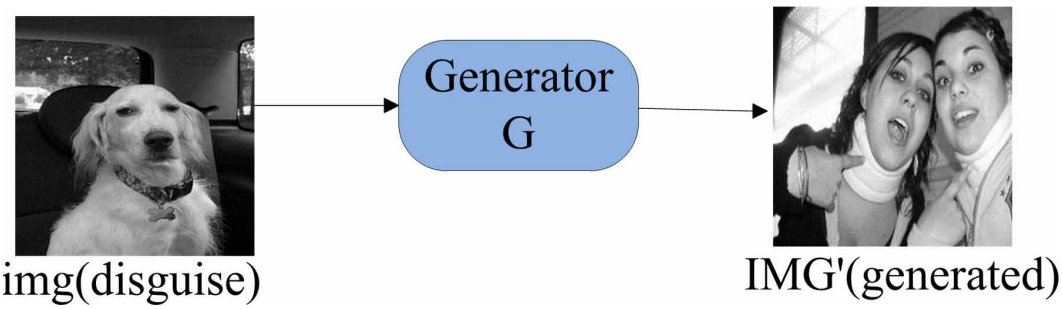


Figure 5. The G model proposed in the paper



passes the img image and the parameters of G to the G, and then produces an IMG' image that is visually the same with the IMG image. The process of experiment is shown in Figure 6.

EXPERIMENTAL RESULTS AND ANALYSIS

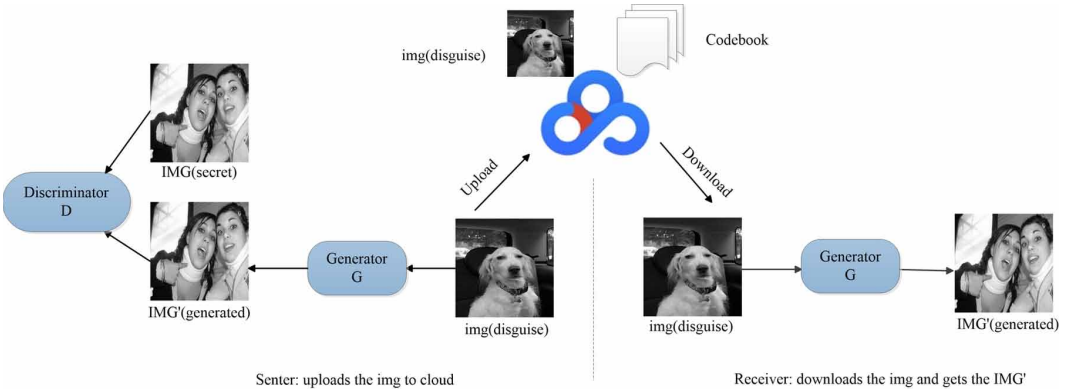
Experimental Environment and Data Sets

Experimental environment is based on the GPU for NIVIDIA GeForce 1080, the version of tensorflow is 1.11.0, and the application is Python 3.5. 100,000 images were extracted from the ImageNet dataset for experiments, including 50,000 images of the img image and the IMG image, and then randomly extracted 1000 images for verification. There are 65536 neurons, 64 neurons and one neuron in input layer, in hidden layer and output layer, respectively of WGAN-GP discriminant network. In the generative network of WGAN-GP model, there are 65536 neurons, 64 neurons and 65536 neurons in the input layer, in the hidden layer and in the output layer, respectively.

Image Quality

Disguised image is regarded as an img image, and the secrect image is regarded as an IMG image. As the number of training increases, as can be seen from Figure 7, a noise image is generated when

Figure 6. The process of experiment



the number of iterations is 1000, and the image contour can be seen when 5000-10000 times. The generated image gradually approaches the IMG image A at 50000 times, and if the number of trainings is enough, the generated image can replace the secret image. The Figure 7 shows the result of the experment.

The receiver inputs the IMG image and the relevant to parameters of the G into G, and the generated IMG' image changes very slightly compared with the original IMG image, which is difficult to distinguish visually. In Figure 8, the first line is the img image, the secondly line is the generated IMG' image, and the third line is the original IMG image.

The IMG' images are visually identical to the IMG image in Figure 8. Moreover visually verifying the four pairs of images exemplified in Figure 8, and 1000 pairs of images were randomly extracted from the ImageNet data set, the histogram analysis of the IMG' and the IMG image is displayed in Figure 9 (a, b, c, d, e, f, g, h).

Peak Signal to Noise Ratio (PSNR) is an objective standard for evaluating images. It is used to measure the quality of processed images (Hore & Ziou, 2010). The PSNR value is usually used to measure the satisfaction of a certain processing program. It is the logarithmic value of the mean square error between the original image and the processed image (the maximum value of the signal is squared, which is the number of bits per sample). Its unit is dB, and the larger the value, the less distortion. The formula for calculating PSNR is as follows:

$$PSNR = 10\log_{10}(\frac{2^n - 1}{MSE}) \tag{10}$$

Figure 7. The process of generating IMG' images as the number of trainings increases

Figure 8. The visual effect of the IMG' image generated after the model is stabilized

Structural Similarity Index (SSIM) is an index to measure the similarity between two images (Bruzzone et al., 2017). Among the two images used in ssim, one is unprocessed image and the other is processed image. The calculation formula of SSIM is as follows:

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^{\ 2}+\mu_y^{\ 2}+c_1)(\sigma_x^{\ 2}+\sigma_y^{\ 2}+c_2)} \tag{11}$$

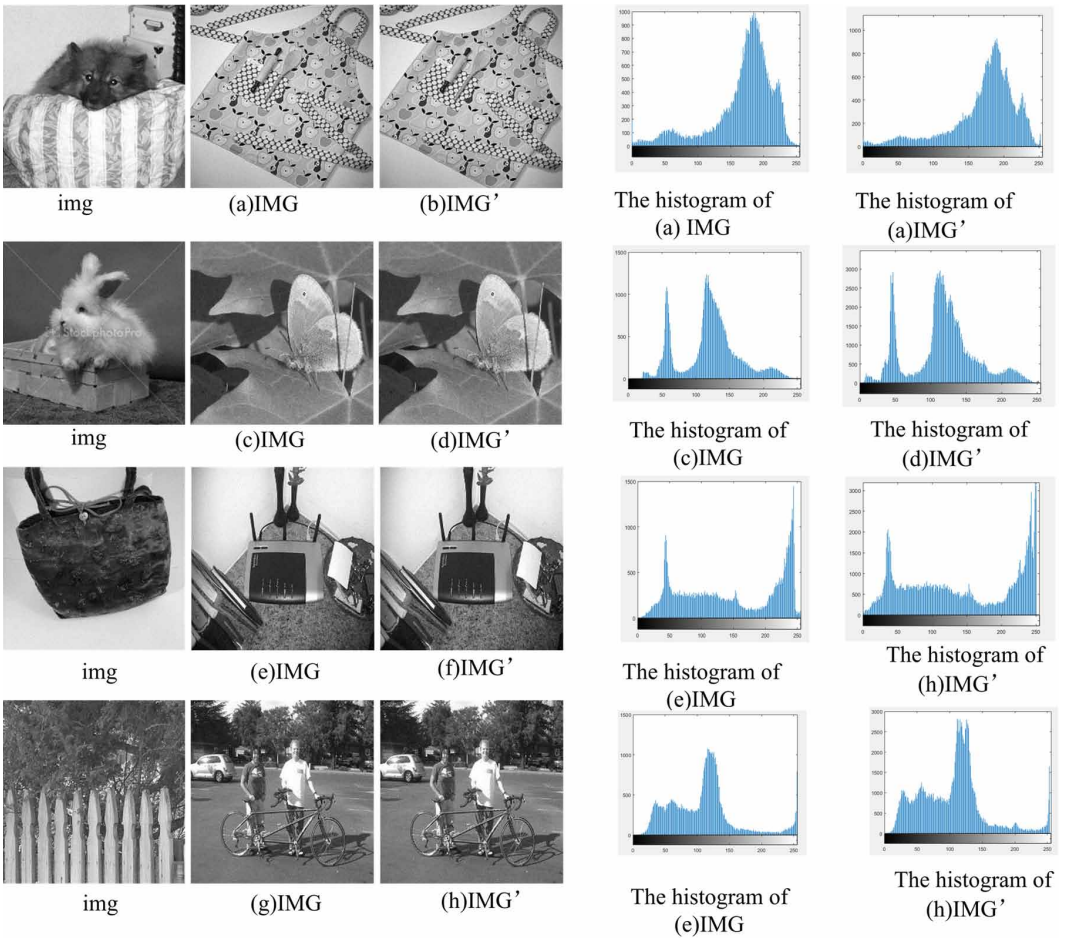
Where μ_x represents the average of x, μ_y is the average of y, $\sigma_x^{\ 2}$ is the square of x, and the variance of $\sigma_y^{\ 2}$ is y, where σ_{xy} is the covariance of x and y. $c_1=(k_1L)^2$ and $c_2=(k_2L)^2$ are constants used to maintain stability. L is the dynamic range of pixel values. $k_1=0.01$, $k_2=0.01$. The value the range of SSIM is (0, 1). The value of SSIM is equal to 1 when the two images are the same (Table 1).

From the sensory effect and error histogram of several a-h images above, the IMG' image is very similar to the IMG image. The PSNR and SSIM values of several images further prove the feasibility of the method.

SECURITY

The img image is transferred to G, the IMG' image is generated, and parameters of the retained generator are transmitted to the G to form different generators for G1, G2...and Gn. The stable generators trained by the img images and the IMG images in Figure 8 are G1, G2, G3 and G4,

Figure 9. Four examples on the ImageNet dataset

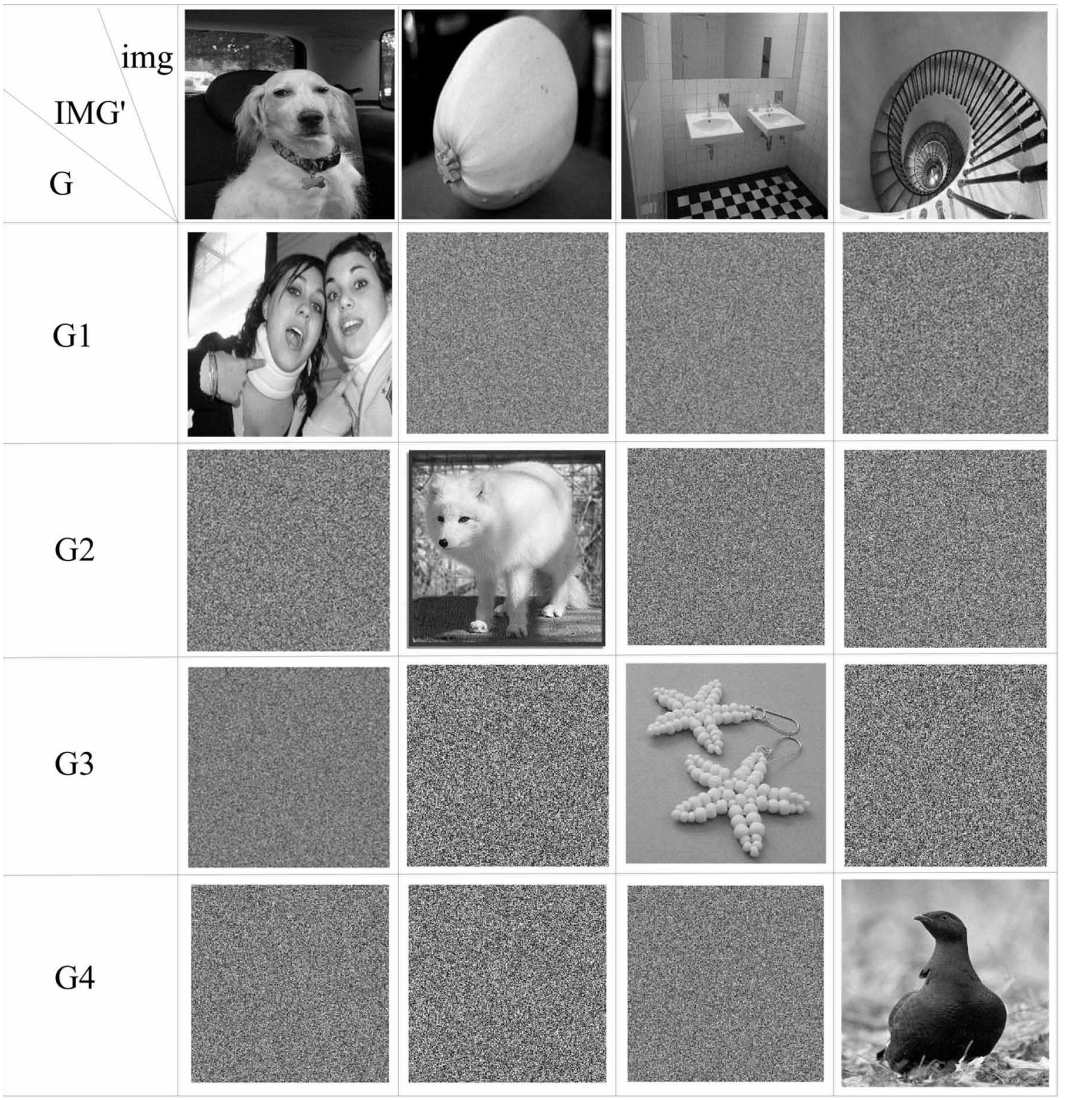


respectively, and the generated images are the IMG' images in Figure 10, respectively. Figure 10 shows that only the img image and its corresponding G can generate image that are visually identical to the IMG image, otherwise only the noise image can be obtained. Only the sender and the receiver have the G. In other words, the attacker can get the IMG' image that is visually same as the secret image only by obtaining the img image and the corresponding G, which verifies the security of the method.

Table 1. Comparison of PSNR(DB) and SSIM values of IMG and IMG'image

Compare Image	PSNR(db)	SSIM
(a)IMG and (b)IMG'	35.0611	0.9362
(c)IMG and (d)IMG'	34.7566	0.9584
(e)IMG and (f)IMG'	33.7891	0.9429
(g)IMG and (h)IMG'	35.1429	0.9457

Figure 10. Security verification



CONCLUSION

The method uses the WGAN-GP network for information hiding. The receiver only needs to download the disguise image, obtains the corresponding parameters of generator from the codebook data, and passes the disguise image and the parameters of generator to the generator to output an image, could realize the same results as sending the secret image. The results of the experimental show that the method has a well effect on the quality of the image and safety of the communication. But the disadvantage is that each disguise image corresponds to a generation model, and the shortcomings of this model will be improved in combination with the encryption algorithm in the next work.

ACKNOWLEDGMENT

The paper was supported by the National Natural Science Foundation of China (No. 61672354), the Key Programs for Science and Technology Development of Henan Province (No. 172102210335), and Key Scientific Research Projects in Henan Province (No.16A520058, 19B510005, 18A510014) we would like to thank the anonymous reviewers for their valuable suggestions.

REFERENCES

Arjovsky, M., Chintala, S., & Bottou, L. (2017). *Wasserstein gan.* arXiv preprint arXiv:1701.07875.

Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, *37*(3), 469–474. doi:10.1016/j.patcog.2003.08.007

Chaumont, M., & Puech, W. (2006, September). A DCT-based data-hiding method to embed the color information in a JPEG grey level image. In *2006 14th European Signal Processing Conference* (pp. 1-5). IEEE.

Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1996, September). Secure spread spectrum watermarking for images, audio and video. In *Proceedings of 3rd IEEE International Conference on Image Processing* (Vol. 3, pp. 243-246). IEEE. doi:10.1109/ICIP.1996.560429

Dang, P. P., & Chau, P. M., (2000). Image encryption for secure internet multimedia applications. *IEEE Transactions on Consumer Electronics, 46*(3).

Deng, J., Dong, W., Socher, R., Li, L. J., Li, K., & Li, F. F. (2009, June). Imagenet: A large-scale hierarchical image database. In 2009 IEEE conference on computer vision and pattern recognition (pp. 248-255). IEEE. doi:10.1109/CVPR.2009.5206848

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*.

Gulrajani, I., Ahmed, F., Arjovsky, M., Dumoulin, V., & Courville, A. C. (2017). Improved training of wasserstein gans. *Advances in Neural Information Processing Systems*, 5767–5777.

Guo, Q., Liu, Z., & Liucora, S. (2011). Image watermarking algorithm based on fractional fourier transform and random phase encoding. *Optics Communications*, *284*(16-17), 3918–3923. doi:10.1016/j.optcom.2011.04.006

Hemalatha, S., Acharya, U. D., & Renuka, A. (2013). A Secure Color Image Steganography In Transform Domain. *International Journal on Cryptography & Information Security, 3*(1).

Holub, V., & Fridrich, J. (2012, December). Designing steganographic distortion using directional filters. In *2012 IEEE International workshop on information forensics and security (WIFS)* (pp. 234-239). IEEE. doi:10.1109/WIFS.2012.6412655

Holub, V., Fridrich, J., & Denemark, T. (2014). Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*, *2014*(1), 1. doi:10.1186/1687-417X-2014-1

Hore, A., & Ziou, D. (2010, August). Image quality metrics: PSNR vs. SSIM. In *2010 20th International Conference on Pattern Recognition* (pp. 2366-2369). IEEE.

Khan, K., Shaheen, M., & Wang, Y. (2018). Using Sparse Matrices to Prevent Information Leakage in Cloud Computing. In *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud).* IEEE Computer Society. doi:10.1109/FiCloud.2018.00070

Liang, G. L., Wang, S. Z., & Zhang, X. P. (2007). Steganography in binary image by checking data-carrying eligibility of boundary pixels. *Journal of Shanghai University*, *11*(3), 272–277. doi:10.1007/s11741-007-0317-2

Lin, W. H., Horng, S. J., Kao, T. W., Fan, P., Lee, C. L., & Pan, Y. (2008). An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Transactions on Multimedia*, *10*(5), 746–757. doi:10.1109/TMM.2008.922795

Liu, Z., Li, S., Liu, W., Liu, W., & Liu, S. (2013). Image hiding scheme by use of rotating squared sub-image in the gyrator transform domains. *Optics & Laser Technology*, *45*, 45. doi:10.1016/j.optlastec.2012.07.004

Qian, Z., Xu, H., Luo, X., & Zhang, X. (2018). New framework of reversible data hiding in encrypted jpeg bitstreams. *IEEE Transactions on Circuits and Systems for Video Technology*, 1–1.

Qian, Z., & Zhang, X. (2016). Reversible data hiding in encrypted images with distributed source encoding. *IEEE Transactions on Circuits and Systems for Video Technology*, *26*(4), 636–646. doi:10.1109/TCSVT.2015.2418611

Ren, Z. B., Sui, Y. X., & Yang, Y. H., & Yang, H. J. (2002). Study of the MSB Information-hiding Technique in a Carrier Image. *Optics and Precision Engineering*, *10*(2), 182–187.

Sakkara, S., & Somashekar, K. (2012). Integer wavelet based secret data hiding by selecting variable bit length. *International Journal of Computers and Applications*, *48*(19), 7–11. doi:10.5120/7454-0458

Samidha, D., & Agrawal, D. (2013). *Random image steganography in spatial domain.* Academic Press.

Wang, S. Z., Zhang, X. P., & Zhang, K. W. (2002). Steganographic technique capable of withstanding RQP analysis. *Journal of Shanghai University*, *6*(4), 273–277. doi:10.1007/s11741-002-0049-5

Wang, Y., Zheng, D. L., Ju, L., Zheng, D. L., & Wei, Y. G. (2005). The spatial-domain encryption of digital images based on high-dimension chaotic system. In *IEEE Conference on Cybernetics & Intelligent Systems*. IEEE.

Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, *24*(9-10), 1613–1626. doi:10.1016/S0167-8655(02)00402-6

Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, *3*(3), 488–497. doi:10.1109/TIFS.2008.926097

Ye, Y., Shan, J., Bruzzone, L., & Shen, L. (2017). Robust registration of multimodal remote sensing images based on structural similarity. *IEEE Transactions on Geoscience and Remote Sensing*, *55*(5), 2941–2958. doi:10.1109/TGRS.2017.2656380

Zhang, X. P., Qian, Z. X., & Li, S. (2016). Prospect of digital steganography research. *Journal of Applied Sciences (Faisalabad)*, *34*(5), 475–489.

Zhang, G. C., Wang, R. D., & Zhang, Y. J. (2003). Digital image information hiding technology based on iterative blending. *Chinese Journal of Computers.*

Zhou, X., & Chen, J. G. (2006). Information hiding based on double-random phase encoding technology. *Journal of Modern Optics*, *53*(12), 1777–1783. doi:10.1080/09500340600624189

Zhou, Z. L., Cao, Y., & Sun, X. M. (2016). Coverless information hiding based on bag-of-words model of image. *Journal of Applied Sciences (Faisalabad)*, *34*(5), 527–536.

Xintao Duan received the Ph.D. degree from Shanghai University, Shanghai, China, in 2011. He is currently an Associate Professor with the College of Computer and Information Engineering, Henan Normal University. His major research interests include image processing, deep learning, and information security.

Baoxia Li received the B.S. degree from Henan Normal University, China, in 2017. She is currently pursuing the M.S. degree with the College of Computer and Information Engineering, Henan Normal University. Her research interests include image processing, deep learning, and image steganography.

Daidou Guo received the B.S. degree from the Henan Institute of Science and Technology, China, in 2017. He is currently pursuing the M.S. degree with the College of Computer and Information Engineering, Henan Normal University. His research interest includes coverless information hiding.

Kai Jia received the B.S. degree from Pingdingshan University, China, in 2016. He is currently pursuing the M.S. degree with the College of Computer and Information Engineering, Henan Normal University. His research interests include image processing, deep learning, and image steganography.

En Zhang received the Ph.D. degree from the Beijing University of Technology. He held a Postdoctoral position with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. He is currently an Associate Professor with the College of Computer and Information Engineering, Henan Normal University, China. His research interests include outsourcing computation, secure multiparty computation, and rational cryptography.

Chuan Qin received the B.S. degree in electronic engineering and the M.S. degree in signal and information processing from the Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the Faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently a Professor. He was with Feng Chia University, Taiwan, as a Postdoctoral Researcher, from 2010 to 2012. His research interests include image processing and multimedia security. He has published more than 110 papers in these research areas.