

Lossy Compression Tolerant Steganography

Ren-Junn Hwang, Timothy K. Shih, Chuan-Ho Kao and Tsung-Ming Chang

Department of Computer Science and Information Engineering, TamKang University,
Tamsui, Taipei, 251, Taiwan, R.O.C.

Abstract. This paper proposes a lossy compression tolerant steganography. Steganography hides the confidential data secretly. The unauthorized people are difficult to detect hidden data. It provides a secure channel to transmit confidential information. Nowadays, it is a very important technique when we are progressively going to computer network age. There are many researchers purposed steganographies, but most of their techniques cannot tolerate the destruction of lossy compression. In this paper, we propose a novel steganography based on the contrastive relation of the grayscale value of neighboring pixels. It is difficult for the human visual system to detect the difference between original image and one that embedded information based on our steganography. Besides, the embedded data can be extracted correctly from the decompressed stego-image. By our technique, the stego-image can be compressed by the lossy JPEG compression process before transmitting or storing it. This feature will speed up the transmission of the stego-image.

1. Introduction

With the fast development of Internet technologies, the information and digital age is coming. It is the trend toward each behavior and people must use computer and Internet tools to reduce manpower and raise work efficiency. Moreover, for national defense force, we will be faced with the digital war. The fact that cannot be denied is that all of the information and management, arms system, rear supply system and modernized arms are exchanged with digital mold and transported by the network system. "How to transmit the secret information over the network?" is an important problem. We must prevent peeping, copying and altering the data from conspirators. Of course, using cryptography to encrypt and transmit these data is a good method. However, the cipher texts generated the cryptosystem are meaningless random codes. Transmitting meaningless random codes directly is to tell other people that there are very important messages in it and remind conspirators to cut, hack or break these confused codes. Therefore, the pure encryption technology cannot solve the problem of transmitting secret data completely. Even if transmitting encrypted secret data, we hope the unauthorized people will think it is a meaningful and its means are independent of the confidential data. Only authorized receivers can extract real secret messages from this meaningful data. This technology is so called steganography.

Steganography hides the transmitted data in a meaningful but not related text or image. Those unauthorized receivers are unable to detect the hidden data while transmitting. Thus, we can avoid attackers painstakingly to break and to intercept. In

steganography, we randomly select one image (named cover image [7]) and embed data into it. This cover image which embedded with secret data is named stego-image [7]. The human visual system looks this stego-image similar to cover images. It is difficult to detect the difference between the stego-image and the cover-image by the human visual system. For a conspirator, although the stego-image has important data, he cannot find it. Therefore, attackers cannot differentiate those that have embedded with secret data from many of others in the network easily. But for an authorized receiver, he can extract concealed data quickly. In [3][6][9], the authors define the steganography must have the following features:

- Imperceptibly: it is difficult to find the difference when data embedded in the stego-image.
- Readily Extracted: an authorized receiver can extract concealed data quickly.
- High Capacity: embedding the data into the image as many as possible.
- Resistance Removal: data which be embedded in the stego-image cannot be moved.

In steganography, the most common method is Vector quantization[4][5]. It uses codebook which sender and receiver have to process data embedded. First of all, sender cuts the image in which he wants to embed data and the block size is as the same as the size of codebook block. Next, searching the similar block and obtain its index value. After that, encrypt the index value and embed it in the cover image, then transmit it. When receiver receives the stego-image, it will obtain the index value and decryption. Finally, using the index value and codebook to restore data. This method loses data and stego-image cannot resist lossy compression. It is not suitable to embed text.

The other steganographies use image pixels to embed data. In [8], the authors provide a Fixed Range Equalization method. They divide the gray-level value into sixteen areas: [0~15], [16~31], ..., [240~255]. Depending on index value, their method determines a suitable area of the embedded data and selects one value to replace the embedded data. The selected value cannot repeat. For instance, data value is 25, select one point in area 16 to 31 and exchange its value. The other common steganographies are LSB[2][9]. It embeds the data in lower bit that can reduce the influence on image after embedded data. This method is the simplest and most direct one. Moreover, it has biggest embedded capacity. However, the previous methods cannot tolerate lossy compression, for example JPEG. In this paper, we propose a novel steganography. The stego-image based on our method can satisfy the previous features. Besides, although stego-image is processed by lossy compression, the embedded data still can be extracted correctly from the decompressed stego-image. In Section 3, our experimental results show this feature.

2. Steganography based on gray-level pixel value contrastive relation

This section will introduce our steganography based on the contrastive relation of gray-level values of the neighbor pixels. In steganography, there are two important data, one is the embedded data and the other is cover image. In accordance with each

embed data bit, we select one correspond pixel in the cover image. We use the contrastive relation of gray-level values of the selected pixel and its top, bottom, left and right neighbor pixels to keep this embedded data. Some of the contrastive relations of gray-level values do not destroy after lossy compression and decompression process. We can extract them correctly based on the contrastive relations. In Section 3, our experimental result shows that our method is valid. Without loss of the generality, this paper assumes the cover image C is an $m \times n$ gray-level image and the gray-level is 256. The data D , which is embedded in C , we assume it is a g bits stream. We use below expressions to express image C , data D and each pixel separately.

$$C = \{c_{ij} \mid 0 \leq i < m, 0 \leq j < n, c_{ij} \in [0, 255] \}, \quad (1)$$

$$D = \{d_i \mid 0 \leq i < g, d_i \in [0, 1] \}, \quad (2)$$

We introduce our method in the following two phases:

[Embedded data Phase]

Step-E1 : Randomly select one number S .

Step-E2 : Generate g different numbers named $A = \{ a_1, a_2, \dots, a_g \}$ based on the seed S . Each value a_i ranges between 1 and $m \times n$. For any two different integer numbers a_i and a_j in A , their top, bottom, left and right neighbor pixels should be different.

Step-E3 : Decide a threshold value t . According to the value of each d_i bit, we alter some pixels in C as the following steps. C' is the stego-image embedded the data D in C .

Step-E3-1 : Compute $k = a_i \text{ DIV } n$ and $l = a_i \text{ mod } n$. The “ $X \text{ DIV } Y$ ” means the quotient of Y dividing X , and “ $X \text{ mod } Y$ ” means remainder of Y dividing X .

Step-E3-2 : Compute the average value v of the pixel c_{kl} in cover image C and its top, bottom, left and right neighbor pixels' gray-level as $(c_{k-1,l} + c_{k,l-1} + c_{kl} + c_{k,l+1} + c_{k+1,l}) / 5$.

Step-E3-3 : If $d_i = 0$; when $v - c_{kl} \geq t$, keep c_{kl} value, otherwise simultaneously alter c_{kl} value and its top, bottom, left and right neighbor pixels value by the same difference until $v - c_{kl} \geq t$.

If $d_i = 1$; when $v - c_{kl} \leq -t$, keep c_{kl} value, otherwise simultaneously alter c_{kl} value and its top, bottom, left and right neighbor pixels value by the same difference until $v - c_{kl} \leq -t$.

Step-E4: Stego-image C' is the image generated by Step-E3.

Step-E5: Send the seed S by the secret channel.

[Extract Embedded data Phase]

When receiver receives image $C' = \{ c'_{ij} \mid 0 \leq i < m, 0 \leq j < n, c'_{ij} \in [0, 255] \}$, he extracts the embedded data by the following steps.

Step-D1 : Generate the set A based on the seed S as Step-E3.

Step-D2 : Extract each bit d_i based on its correspondence value a_i as the following steps.

Step-D2-1 : Compute $k = a_i \text{ DIV } n$ and $l = a_i \text{ mod } n$.

Step-D2-2 : Compute the average gray-level value v of the image pixel c_{kl} and its top, bottom, left and right neighbor pixels as $(c'_{k-1,l} + c'_{k,l-1} + c'_{kl} + c'_{k,l+1} + c'_{k+1,l}) / 5$.

Step-D2-3 : If $v > c'_{kl}$ then $d'_i = 0$, otherwise $d'_i = 1$.

Step-D3 : Integrate all the bits d'_i extracted by Step-D2, and make up the embedded data D' .

3. Experimental Results and Discussion

This section shows the experimental results of our proposed method. By to this result, we show our method can tolerant JPEG lossy compression and extract the embedded data correctly. Thus, our novel technique not only provides a way to embed secret data which are not easily to be detected while transmitted by the open channel, but also the stego-image can be compressed by the lossy JPEG compression process.

In our experiment, we select the chapter 3 of the Gospel According to Matthw, shown in Figure 1, as the embedded data. It contains 2056 bytes. We select Lena, F16, Baboon, Boat, Pepper, Sailboat and Toys, shown in Figure 2, as the cover images. They are gray-level 512×512 pixels images. In experimental process, we select 15 as the threshold value t in Step-E4.

The stego-images are shown in Figure 3. Clearly, it is hard to recognize embedded data and their location directly from the stego-image by the human visual system. We use the PSNR (Peak Signal to Noise Ratio) value to evaluate the transparency feature of our method. The PSNR is a popular method to evaluate the difference between the decompressed image and its original image. It's defined as following :

$$\text{MSE} = \left(\frac{1}{m \times n} \right)^2 \sum_{i=0}^{i < n} \sum_{j=0}^{j < m} (c'_{ij} - c_{ij})^2, \quad (3)$$

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \text{ dB}, \quad (4)$$

The c_{ij} and c'_{ij} are pixels in C and C' image. The C and C' are $m \times n$ size images. Generally speaking, if C and C' 's PSNR value larger than 30dB, the human visual is difficult to recognize the difference between C and C' . The first row of Table 1 shows

the PSNR values of the stego-image and its cover-image. All of them are larger than 31 dB. Obviously, there are good transparency features in our proposed method.

To be objective and avoid personal subjective conditions, we use the lossy JPEG function of the PhotoShop 5.0 to compress stego-image. The second row of Table 2 shows the compression ratio (image size/compression image size : 1) of the stego-image in which the embedded data can be extracted from the decompressed stego-image correctly. All of the compression ratio is approximately in 2 : 1. It means that we can reduce the half size of the stego-image before transmitting or storing it.

In Step-E2, we generate a seed S , it likes a secret-key in traditional encryption. If people cannot obtain S , he cannot extract data from stego-image. This shows our method provides a well safety of embedded data. Besides, if we want to intensify the safety of data, the embedded secret data can be processed by encryption and digital signature first, then embedded cipher text in cover image. Our steganography can combine with any encryption and decryption technique and digital signature directly.

4. Conclusion

In this paper, we propose a steganography based on the contrastive relation of the gray-level values of the neighbor pixels. Some of the contrastive relation among the values of the neighbor pixels does not alter after the JPEG lossy compression process. The proposed steganography does not only contain the features as the other steganography, but also can tolerate JPEG lossy compression. When receiver receives the stego-image, he can decompress stego-image and extract the embedded data correctly from it. The transmissions of lossy compressed stego-images are more efficient than the original stego-image. The proposed steganography is more practical than the other steganography.

Acknowledgement

This work was supported in part by the National Science Council of the Republic of China under contract NSC89-2218-E-032-027.

References

- [1] The New Testament Revised Standard Version And Chinese Union Version: The Gospel According to Matthew Chapter3, pp. 5-7 (1985)..
- [2] E. Adelson (1990), "Digital Signal Encoding and Decoding Apparatus," *U.S. Patent, No.4939515*.
- [3] W. Bender, D. Gruhl, N. Morimoto, and A. Lu (1996), "Techniques for Data Hiding," *IBM Systems Journal*, Vol. 35, Nos 3 and 4, pp.313-336.
- [4] T. S. Chen, C. C. Chang, and M. S. Hwang (Oct.1998), "Virtual Image Cryptosystem Based upon Vector Quantization," *IEEE Transactions on Image Processing*, Vol. 7, No. 10, pp.1485-1488.

- [5] T. S. Chen, and Y. H. Hsu (1997), "Image Camouflage and Encryption Method Using Vector Quantization," *The Second Conference of Information Management and Its Application in Law Enforcement*, Taipei, R.O.C., pp.97-106.
- [6] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoan (September 1996), "Secure Spread Spectrum Watermarking for Images, Audio and Video," *Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland*, pp.243-246.
- [7] N. F. Johnson and S. Jajodia (Feb. 1998), "Exploring Steganography: Seeing the Unseen," *IEEE Computer Magazine*, Vol. 31, NO. 2, pp.26-34.
- [8] M. S. Liaw and L. H. Chen (Nov. 1997), "An Effective Data Hiding Method," *Proceeding of the Sixth National Conference on Science and Technology of National Defense*, Vol. 2, Taoyuan, Taiwan, pp.534-540.
- [9] Lisa M. Marvel, Charles T. Retter and Charles G. Boncelet (1998), "Hiding Information in Images," in *Proceedings of ICIP*.

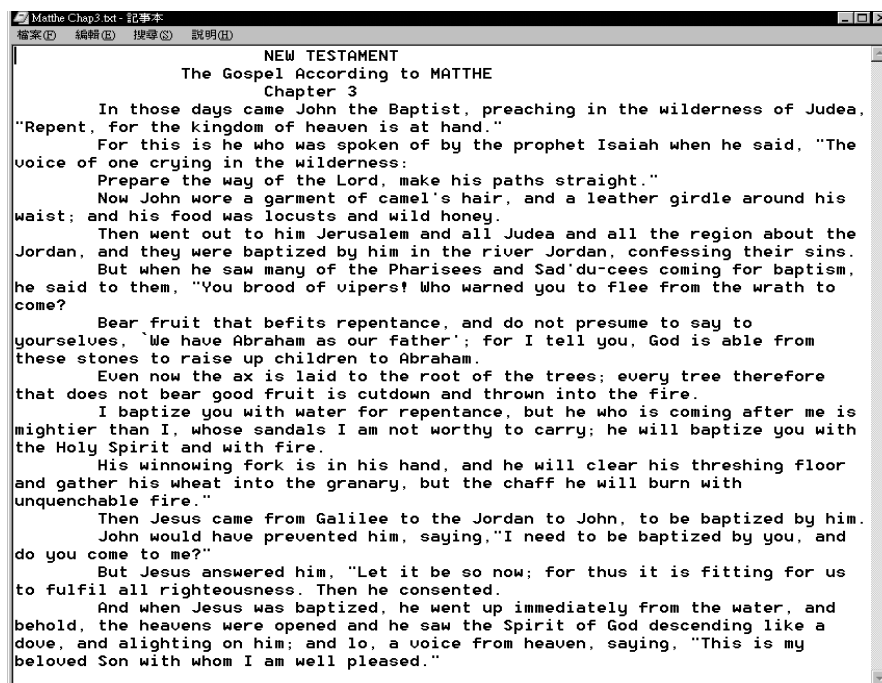


Fig. 1. The chapter 3 of the Gospel According to Matthe



(a) Lena



(b) F16



(c) Baboon



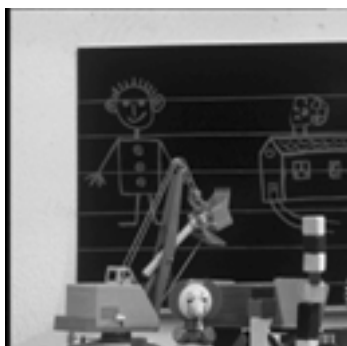
(d) Boat



(e) Pepper

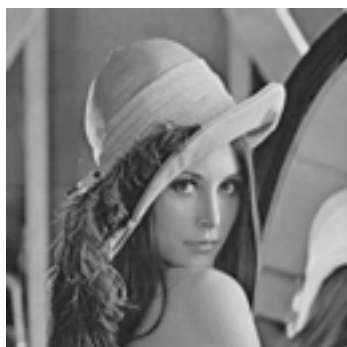


(f) Sailboat



(g) Toys

Fig. 2. 512×512 cover image



(a) Lena



(b) F16



(c) Baboon



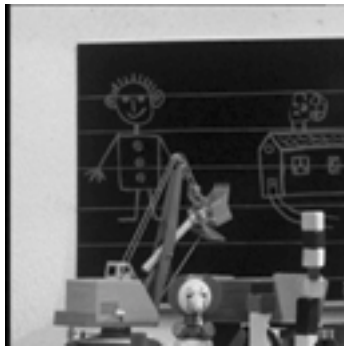
(d) Boat



(e) Pepper



(f) Sailboat



(g) Toys

Fig. 3 512×512 Stego-image

Table 1. Each image's PSNR value and can extracted 100% compression ratio after embedded Fig. 1 data

	Lena	F16	Baboon	Boat	Sailboat	Toys
PSNR value	33.07	33.03	31.72	32.84	32.71	32.93
Compression ratio	2.42 : 1	2.39 : 1	2.05 : 1	2.31 : 1	2.12 : 1	2.44 : 1