Secure RGB Image Steganography based on Fused Distortion Measurement

A. Antony Raj[1], M. Vickraman[2], A. Vishnu[3], M. R. Mahalakshmi[4]
[1,2,3]*Student, Dept. of Electronics and Communication Engg., Sri Muthukumaran Inst. of Tech., Chennai, India*
[4]*Professor, Dept. of Electronics and Communication Engg., Sri Muthukumaran Inst. of Tech., Chennai, India*

Abstract**: Binary image Steganographic methods aim to generate stego images with good visual quality, while others focus more on the statistical security of the anti-steganalysis. This paper proposes a binary steganographic scheme that improves both of them by selecting more appropriate flipped pixels. First, a fused distortion measurement is developed that combines the advantages of flipping distortion measurement (FDM) and two data-carrying pixel location methods, including the edge adaptive grid method (EAG) and the "Connectivity Preserving" criterion (CPc). The FDM measures the distortion score by statistical features and achieves high statistical security, while the EAG and CPc select pixels by analysing local texture structures based on visual quality. Then, to eliminate the interference brought by adjacent flipped pixels, a flipping position optimization strategy is proposed to find better positions for flipping pixels to further improve the steganographic performance.**

Keywords: **Binary image steganography; visual quality, statistical security of anti-steganalysis; fused distortion measurement; flipping position optimization**

1. Introduction

Steganography is a way of transmitting secret messages under digital media in public channels. Only the sender and the receiver can extract the secret messages from the digital media. Binary images (including signatures, handwritings, CAD graphs, and cartoon images) can be seen everywhere and have a wide usage in our daily life, such as in facsimile communication. Steganography in binary images is becoming increasingly more significant. However, unlike grayscale images, pixels in binary images only have two values: "1" and "0". When embedding secret messages in binary images in the spatial domain, pixels should be directly flipped to carry some messages, which will lead to visual distortion on binary images and may be easily detected, even by human eyes. Furthermore, stego images may be attacked by some existing steganalysis methods. Therefore, the statistical security of anti-steganalysis is another important aspect that should be considered in binary image steganography. As a result, we should consider both of them when hiding data in binary images. A steganographic scheme with better visual quality and stronger statistical security is required.

In this paper, we proposed a steganographic scheme focusing on both visual quality and the statistical security of anti-steganalysis. We first combine the merits of two previous data-carrying pixel location methods and the flipping distortion measurement to construct a fused distortion measurement that more accurately selects flippable pixels. Furthermore, considering that flipping a pixel may influence the flippability of its adjacent pixels, flipping position optimization is proposed to optimize the flipping positions to eliminate the interference.

To improve the statistical security of anti-steganalysis, we proposed a spatial-domain-based binary image steganographic scheme based on the statistics of local texture patterns. A complement, rotation, and mirroring-invariant Local Texture Pattern (crmiLTP) was defined to describe the textures of binary images, which was also used to compute the distortion score of each pixel and rank the flipping priority of each pixel. The distortion measurement they proposed assessed the change in the number of crmiLTPs and the sensitivity of crmiLTPs in different embedding types. In the embedding procedure, Syndrome-Trellis Codes (STC) was employed to minimize the flipping distortion and achieve a relatively large payload. By the statistical distortion measurement and STC, the scheme achieves strong statistical security.

2. The proposed steganographic scheme

In this section, we will introduce the proposed steganographic scheme in details. First, a fused distortion measurement is developed to better measure the distortions brought by flipping pixels. Then, flipping position optimization is designed to find better flipping positions for flipping pixels to embed secret messages. Finally, the total embedding and extraction procedures will be discussed in the last subsection.

A. Constructing a fused distortion measurement

Some distortion measurements concentrate on establishing good stego image quality, while others aim at establishing strong statistical security. To construct a distortion measurement to better measure the distortions brought by flipping pixels, we combine the merits of the flipping distortion measurement (FDM) and two data-carrying pixel location methods (including the edge adaptive grid method (EAG)and the "Connectivity Preserving" criterion (CPc)) to design a fused distortion measurement. The distortion score of FDM is computed by

$$D_{i,j} = (\sum_{t=0}^{255} W_t |\, H_t^X - H_t^{Y_{i,j}}|)^{\alpha} + \beta$$

Where, X denotes the cover image and $Y_{i;j}$ denotes the stego image generated by flipping the pixel located at ($i; j$). t denotes the value of crmiLTP, W_t denotes the weight of crmiLTP computed by Fisher's criterion [12], and t and W_t are calculated according to [10]. H_t^X and $H_t^{Yi;j}$ denotes the total number of crmiLTPs whose values equal t in image X and $Y_{i;j}$, respectively. α and β are used to control the sensitivity. We use EAG and CPc to locate the boundary pixels in the cover image X. The boundary pixels found by EAG are denoted as $P_1 = \{p_e\}$, where e = 1, 2, 3….m and m is the total number of boundary pixels found by EAG. The boundary pixels found by CPc are denoted as $P_2 = \{p_c\}$, where c = 1, 2, 3...n and n is the total number of boundary pixels found by CPc. To make flippable pixels more focused on boundaries, the distortion scores of these boundary pixels found by EAG and CPc should be further reduced. The proposed distortion measurement is computed by

$$D'_{i,j} = \{^{(\sum_{t=0}^{255} W_t|H_t^X - H_t^{Y_{i,j}}|)^{\alpha} + \beta, \qquad p_{i,j} \in \{p_e, p_c\}}_{\gamma[(\sum_{t=0}^{255} W_t|H_t^X - H_t^{Y_{i,j}}|)^{\alpha} + \beta \qquad p_{i,j} \in \{p_e, p_c\}}\}$$

$$D''_{i,j} = trunc_t(D'_{i,j}) = \{^{T, \quad D'_{i,j} < T}_{D'_{i,j}, \quad D'_{i,j} >= T}$$

Where $D_{i;j}{}''$ is the distortion score after truncating, $D_{i;j}{}'$ denotes the distortion score of the pixel ($i; j$). The procedures of distortion measurement selection strategy used in each image block are as follows:

- For the i-th image block, Eq. (1) and Eq. (3) are used to compute the distortion scores of pixels, respectively.
- In the i-th image block, these two distortion scores are used to embed the same secret message segment, respectively. Then, two stego images can be obtained.
- The visual quality and the number of flipped pixels are compared in these two stego images. Finally, in the i-th image block, the distortion measurement that can produce the stego image with better visual quality and fewer flippable pixels is chosen to embed the message segment.
- Repeat Step 1 to Step 3 until all image blocks have been considered.

The distortion measurement selection strategy selects the most suitable distortion measurement in each image block. This strategy ensures that the number of flipped pixels in each image block is the least. Therefore, it solves the second problem mentioned above and further improves the visual quality of stego images.

B. Flipping position optimization

Considering that flipping a pixel may influence the flippability of pixels around it, the distortion scores of adjacent pixels will be changed and may no longer be suitable for flipping. As a result, simultaneously flipping adjacent pixels may degrade the visual quality and statistical security of stego images. In the embedding procedure, scrambling and STC are used to embed secret messages. However, these two methods do not consider the interference among flipped pixels. As shown in Section III-D, without eliminating the interference, some undesirable pixels may be flipped to embed secret messages. To eliminate the interference, a flipping position optimization (FPO) strategy is proposed to find better flipping positions to achieve better visual quality and higher statistical security. To not influence the extraction procedure, the candidates of flipping positions we found were those came from the same super pixel and FPO is used in these candidates to achieve the best flipping positions.

- The procedures of the FPO are as follows:
- Obtain the positions of flipped pixels from the stego image Y and the cover image X. The positions of flipped pixels are denoted as $C = f\{_b\}$, here b = 1,2,3… k and k is the number of flipped pixels.
- Calculate the distortion score D_Y of the stego image Y using Eq. (1).
- For each flipped pixel c_b, find the pixels that come from the same super pixel. Among the pixels, we further find the pixel with the lowest distortion score and denote it as p_{lowest}. If p_{lowest} is the same pixel as c_b, c_b is selected to flip. If p_{lowest} is not the same pixel as c_b, use the objective visual quality measurements (introduced in Section III-B) to determine which pixel to flip to achieve better visual quality.
- Repeat Step 3 until all the flipped pixels have been considered.

C. General framework of embedding and extraction

Based on the proposed fused distortion measurement and flipping position optimization strategy, the steganographic scheme is constructed in this part. It consists of embedding and extraction procedures.

- *Embedding Procedures:* Given a binary cover image X of size l_w l_h, we divide X into non-overlapped blocks of size l' l'. Suppose the length of each message segment is l_m. By changing l_C and l_I, we can achieve different stego images with different lengths of embedded messages. The embedding procedure includes the following steps:

Calculate the distortion score map of image X (denoted as D) by using Eq. (1).

- Use the edge adaptive grid method (EAG) to find the positions of boundary pixels denoted as $P_1 = \{p_e\}$, where e = 1,*2,3…m* and m is the number of boundary pixels found by EAG. Use the "Connectivity

Preserving” criterion (CPc) to find another position of boundary pixels denoted as P_2 = {p_c}, where c = 1,2,3… n and n is the number of boundary pixels found by CPc. Then, Eq. (3) is used to calculate the fused distortion score map of cover image X (denoted as D'').

- Divide X, D and D'' into non-interlaced image blocks of size l' l', where l' = l_C l_I. Divide secret messages m into non-overlapped message segments of length l_m.
- Use the image block selection method proposed in to select all the proper non uniform blocks in X (denoted as eX), the corresponding distortion score blocks in D (denoted as eD), and the corresponding distortion score blocks in D'' (denoted as eD''). Scramble eX, eD and eD'' with the same scrambling seed so that each scrambled pixel still corresponds to the correct distortion score at the same location. The scrambled image and two distortion scores are denoted as sX, sD and sD''.
- For the i-th image block, the distortion measurement selection strategy mentioned in Section II-A is used to choose the most suitable distortion score block from the i-th score blocks of sD and sD''. The selected distortion score block is denoted as bD.
- Divide the i-th image block into superpixels of size l_I l_I. The value of each superpixel is determined by the parity of the black pixels in it. The value of a superpixel is equal to “1” if the number of black pixels in that superpixel is odd and the value of a superpixel is “0” if the number of black pixels is even. The corresponding distortion score of each superpixel is defined as the lowest score in it. These l_C l_C superpixels are used as a cover vector to embed the i-th message segment by applying the STC encoder.

D. *Embedding*

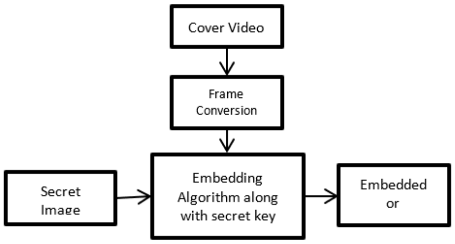

Fig. 1. Embedding

E. *Extraction*

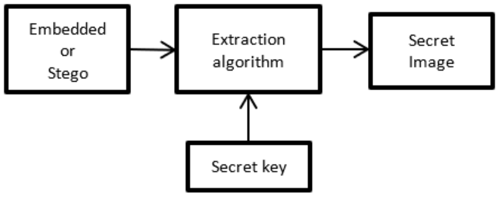

Fig. 2. Extraction

- For each super pixel whose value needs to be changed, flip the pixel with the lowest distortion score in it.
- Repeat Steps 5 to 7 until all the message segments have been embedded.
- Descramble the embedded image blocks.
- Successively replace each non uniform block in the cover image with the corresponding stego block to obtain the stego image Y.
- Use the flipping position optimization to generate a new stego image Y'.

Extraction Procedures: In the extraction procedure, l_C, l_I, l_m, and the scrambling seed are necessary to construct the same STC. The detail of the extraction procedures are as follows:

- Divide the stego image Y' into non-overlapped blocks of size l' l', where l' = l_C l_I. Select all the non-uniform image blocks, denoted as Y''.
- Use the same random sequence in Step 4 of the embedding procedure to scramble Y''

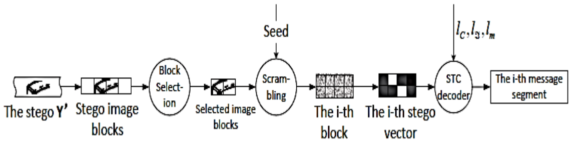

Fig. 3. Extraction procedures

- For the i-th stego image block, form the l_C l_C length stego vector by using the same process in Step 6 of the embedding procedure. Employ the stego vector to extract the i-th message segment by applying the STC decoder.
- Repeat Step 3 until all the message segments have been extracted.

3. Experiment results

A. *Image dataset*

This paper use BIVC (Binary Images comprised of Various Contents) dataset to compare the performance of different steganographic schemes. The BIVC dataset consists of 5000 binary images of size 256x256.

Fig. 4. Cover video

Fig. 5. Frame selection

Fig. 6. Secret image

Fig. 7. Embedded image

4. Conclusion

In this paper, we first briefly review the development process of binary steganography and analyse some state-of-the-art binary image steganographic schemes. We find that visual quality is especially important in binary images, and a practical binary steganography should consider both the visual quality and statistical security of anti-steganalysis. To this end, we propose a fused distortion measurement using both global statistical characteristics and local structured features. We combine the merits of FDM and two data-carrying pixel location methods including EAG and CPc. FDM focuses on the statistical security and measure the distortion scores by statistical characters, while EAG and CPc focus on the visual quality and select flippable pixels by local structured features. Experiments show that the performance of the fused distortion measurement we propose is better than other state-of-the-art distortion measurements. Furthermore, to eliminate the interference between flipped pixels, we propose a flipping position optimization (FPO) to find better positions for flipping to further improve the steganographic performance. Finally, a practical steganographic scheme is proposed. Experimental results show that the stego images generated by the proposed scheme have better visual quality and stronger statistical security compared with the state-of-the-art steganographic methods.

Research into improving steganographic performance in binary images is still in progress. In this work, we review the previous schemes and find that considering only one aspect of visual quality and statistical security is not enough. We propose a scheme focusing on both of them and achieve high steganographic performance, which confirms our mentioned discovery. Again, we think that a practical binary steganography should consider both visual quality and statistical security of anti-steganalysis. In the further research, we will further study the visual quality and statistical security in binary images. We aim to reveal the deep relationship between them to design a better scheme and improve the steganographic performance.

References

[1] Adrian Hernandez-Becerril, Mariko-Nakano-Miyatake, Marco Ramirez-Tachiquin, Hector Perez-Meana (2013), “A Parallel Implementation of Multiple Secrete Image Sharing Based on Cellular Automata with LSB Steganography”, 12th IEEE International Conference on Intelligent Software Methodologies, Tools and Techniques, pp. 25-26.

[2] Bingwen Feng, Wei Lu, Wei Sun (2013) “Secure Binary Image Steganography Based on Minimizing the Distortion on The Texture”, IEEE Transactions on Information Forensics and Security, pp.1-18.

[3] Christopher N. Gutierrez, Gautam Kakani, Ramesh C. Verma (2010), “Digital Watermarking of Medical Images for Mobile Devices”, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp 56-58.

[4] Hossein Nezamabadi, Mohadeseh Soleimanpour,Malihe M. Farsangi, Maryam Mahyabadi (2012), “A more secure steganography method based on pair-wise LSB matching via a quantum gravitational search algorithm”, The 16th CSI International Symposium on Artificial Intelligence and Signal Processing, pp. 25-28.

[5] Pauline Puteaux and William Puech (2018) “An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images”, IEEE Transactions on Information Forensics and Security, pp.5-7.

[6] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma (2013) “A Secure Video Steganography with Encryption Based on LSB Technique”, International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2, pp. 25-29.

[7] Sharafat Hossain, Masud an Nur Islam Fahim (2017), “A Simple Way of Image Encryption Using Pixel Shuffling and Pixel Manipulation”, 20th International Conference of Computer and Information Technology (ICCIT), pp. 89-92.

[8] S. Thenmozhi, M. Chandrasekaran (2012), “Novel Approach for Image Stenography Based on Integer Wavelet Transform”, IEEE, pp.159-162.

[9] Volkan Kaya, Ersin Elbasi (2018) “Robust Medical Image Watermarking Using Frequency Domain and Least Significant Bits Algorithms”, IEEE, pp.125-128.

[10] Xiang Zhang, Fei Peng, and Min Long (2018) “Robust Coverless Image Steganography based on DCT and LDA Topic Classification”, IEEE Transactions on Multimedia, pp. 15-18.

[11] Yu-Chee Tseng, Yu-Yuan Chen, and Hsiang-Kuang Pan (2002), “A Secure Data Hiding Scheme for Binary Images”, IEEE Transactions on Communications, vol. 50, no. 8, pp. 22-25.

[12] https://en.wikipedia.org/wiki/Steganography