 CMC, vol.59, no.3, pp.943-953, 2019

Distortion Function for Emoji Image Steganography

Lina Shi[1], Zichi Wang[1], Zhenxing Qian[1,*], Nannan Huang[1], Pauline Puteaux[2] and Xinpeng Zhang[1]

Abstract: Nowadays, emoji image is widely used in social networks. To achieve covert communication in emoji images, this paper proposes a distortion function for emoji images steganography. The profile of image content, the intra- and inter-frame correlation are taken into account in the proposed distortion function to fit the unique properties of emoji image. The three parts are combined together to measure the risks of detection due to the modification on the cover data. With the popular syndrome trellis coding (STC), the distortion of stego emoji image is minimized using the proposed distortion function. As a result, less detectable artifacts could be found in the stego images. Experimental results show that the proposed distortion function performs much higher undetectability than current state-of-the-art distortion function HILL which is designed for natural image.

Keywords: Steganography, emoji image, distortion function.

1 Introduction

Data hiding embeds additional data into digital media without causing seriously distortion to guarantee the usability of cover object [Dong, Zhang and Liu (2018); Qian, Xu, Luo et al. (2018); Qian and Zhang (2016)]. The purposes of data hiding are covert communication and copyright protection usually [Qian, Zhang and Wang (2014); Qian, Zhou, Zhang et al. (2016); Wang, Qian, Zhang et al. (2018)]. To achieve covert communication, steganography aims to embed secret data into digital media without drawing suspicion by slightly modifying cover data [Li and Zhang (2019); Wang, Zhang and Yin (2018); Wang, Yin and Zhang (2019)]. Early works by Fridrich et al. [Fridrich and Soukal (2006); Zhang and Wang (2006); Zhang, Zhang and Wang (2008)] increasing the undetectability of steganography by decreasing the quantity of modifications on cover data. However, the undetectability is not satisfactory since the security performance of steganography is also related to the modified locations. The currently popular approach by Fridrich et al. [Fridrich and Filler (2007)] is to minimize the additive distortion between the cover and the stego objec, which is achieved by syndrome trellis coding (STC) [Filler, Judas and Fridrich (2011)]. In this framework, a user-defined distortion

[1] Shanghai Institute for Advanced Communication and Data Science, School of Communication and Information Engineering, Shanghai University, Shanghai, 200444, China.

[2] Laboratoire d'Informatique, de Robotique et de Microlectronique de Montpellier, Centre National de la Recherche Scientifique, University of Montpellier, Montpellier, 34095, France.

[*] Corresponding Author: Zhenxing Qian. Email: zxqian@shu.edu.cn.

function is used to assign embedding costs for all cover elements to quantify the effects of modification. There are many distortion functions designed for spatial images, such as Holub et al. [Holub and Fridrich (2012); Holub, Fridrich and Denemark (2014); Li, Wang, Huang et al. (2014); Sedighi, Cogranne and Fridrich (2016)] and JPEG images, such as Guo et al. [Guo, Ni and Shi (2014); Guo, Ni, Su et al. (2015); Wang, Zhang and Yin (2016); Wei, Yin, Wang et al. (2018); Du, Yin and Zhang (2018)].

For other kinds of images, new distortion functions should be proposed to fit their unique properties. In the age of big data currently, many kinds of digital images [Guan, Zhang, Wu et al. (2019); Wu, Dong, Ota et al. (2018)] are emerged. Specially, emoji image is widely used in social networks, e.g., Twitter, Facebook, and instant messaging systems, e.g., Skype, WeChat, to express emotion vividly. Different with natural image, as shown in Fig. 1, the emoji image is constituted by several curves with legible profile. The correlation between pixels is different from natural image which can be modeled as Markov chain. To save storage space, the usual format of emoji image is palette (a typical example: graphics interchange format). For the vitality of expression, most of the emoji images are motional. That means there are more than one frame contained in each emoji image. In this case, the correlation between the frames should also be considered for steganography. Furthermore, this inter-frame correlation is different from the correlation in natural images which are motionless.

Figure 1: Several emoji images

Existing distortion functions [Holub and Fridrich (2012); Holub, Fridrich and Denemark (2014); Li, Wang, Huang et al. (2014); Sedighi, Cogranne and Fridrich (2016); Guo, Ni and Shi (2014); Guo, Ni, Su et al. (2015); Wang, Zhang and Yin (2016); Wei, Yin, Wang et al. (2018)] are designed for natural image, which aim to restrain embedding changes into texture and complex regions to conceal the modification trace [Wang, Yin and Zhang (2018)]. Although these distortion functions perform well in natural image, they are not suitable for emoji image since the profile has not been used enough. Therefore, it is necessary to develop customized distortion function for emoji image. To the best of our knowledge, there is no distortion function designed for emoji image.

To fill up this gap, we propose a distortion function for steganography in emoji image. Different with existing distortion functions designed for natural image, the proposed distortion function combines the profile of image content, the intra- and inter-frame correlation together to measure the risks of detection due to the modification on the cover data. In this way, the unique properties of emoji image are considered. When secret data is embedded with syndrome trellis coding, the obtained stego emoji exposes less detectable artifacts.

2 Structure

The structure of the proposed method is shown in Fig. 2. To fit the properties of emoji image, the profile of image content, the intra- and inter-frame correlation are employed to form the profile, texture, and variation cost respectively. Then the three parts are combined together to measure the risks of detection due to the modification on the cover data.

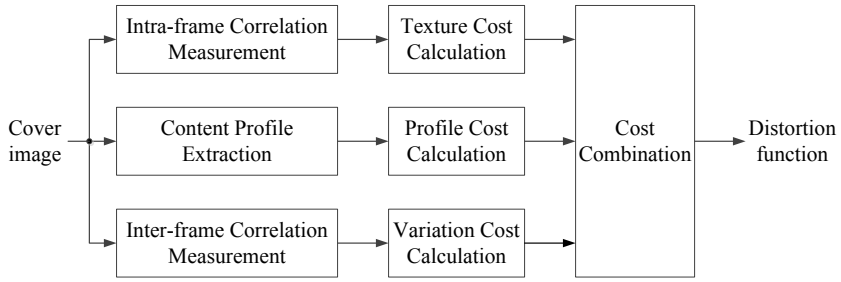


Figure 2: Structure of the proposed distortion function

2.1 Emoji image

The usual format of emoji image is palette. As shown in Fig. 3, each palette image is composed of a color palette and a color index matrix. The color palette is a list of entries of representative colors in the image, and the elements in the color index matrix are pointers to those palette entries that specify the red-green-blue (RGB) colors [Tzeng, Yang and Tsai (2004)].

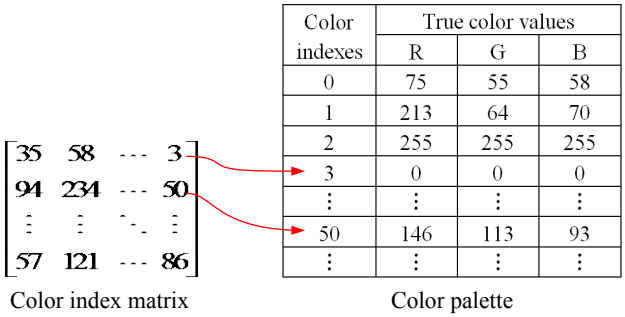


Figure 3: Demonstration of the palette format

Since there is more than one frame (color index matrix) contained in each emoji image, each emoji image is composed of a color palette and several color index matrices corresponding to the frames. In other words, an emoji image is composed of several palette images with only one-color palette. The color palette is shared with all color index matrices.

2.2 Distortion function design

According to the properties of the emoji images, a new distortion function is designed. For an emoji image with k colors and l color index matrices, denote the i-th index in color palette as c_i, $i \in \{0, \ldots, k\}$, the j-th color index matrix with size $M \times N$ as $\mathbf{X}_j = \{x_j(u,v)\} \in$

$\{c_i\}^{M\times N}$, $j\in\{0, \dots, l\}$. The proposed distortion function assigns a embedding cost for each $x_j(u,v)$. The details are as follows.

Denote the RGB color values corresponding to c_i as R_i, G_i, and B_i respectively. To minimize the color value distortion cause by the modifications made on $x_j(u,v)$ during steganography, the value-similar $x_j(u,v)$ should corresponding to similar (R_i, G_i, B_i) values. To achieve this, all the $\mathbf{X}_j$ are modified using Algorithm 1.

Algorithm 1 Color index matrix adjustment

Input: The j-th color index matrix $\mathbf{X}_j$, color palette c_i.

Output: Adjusted $\mathbf{X}_j$.

(1) Find all the minimal $x_j(a_0,b_0)$ in $\mathbf{X}_j$, $a_0\in\{1, \dots, M\}$, $b_0\in\{1, \dots, N\}$, then set all $x_j(a_0,b_0)$ as 0;

(2) Calculate $\theta_i=R_i^2+G_i^2+B_i^2$ for all the $M\times N$ $x_j(u,v)$.

(3) Set w=1;

(4) Find all $x_j(a_w,b_w)$ with the most similar θ_i with $x_j(a_{w-1},b_{w-1})$, then set all $x_j(a_w,b_w)$ as w;

(5) Repeat step (4) for all the cases of $w > 1$ until all the $x_j(u,v)$ in $\mathbf{X}_j$ are adjusted.

The first part of the proposed distortion function aims to take use of the intra-frame correlation. This purpose is similar with the distortion functions for natural images. Current state-of-the-art distortion function is HILL, which constituted by a high-pass filter and two low-pass filters to make the modifications clustered. We employ the approach of HILL to assign the texture cost $\rho_j^{\mathrm{T}}(u,v)$ for each $x_j(u,v)$. The details are as follows.

Let $\mathbf{F}_{\mathrm{h}}$ be a high-pass filter, the residuals $\mathbf{R}_j$ of $\mathbf{X}_j$ are calculated using Eq. (1) firstly.

$$\mathbf{R}_j=\mathbf{X}_j\otimes\mathbf{F}_{\mathrm{h}} \tag{1}$$

where

$$\mathbf{F}_{\mathrm{h}}=\begin{bmatrix}-1 & 2 & -1\\ 2 & -4 & 2\\ -1 & 2 & -1\end{bmatrix} \tag{2}$$

The nonexistent pixel which is out of the image boundary would be obtained by pixel symmetric padding. For example, $x_j(u+1,v)$ is obtained by copying $x_j(u-1,v)$ when it is out of the block boundary, and vice versa. Then two low-pass filters $\mathbf{F}_{l1}$ and $\mathbf{F}_{l2}$ are employed to obtained the cost matrix $\boldsymbol{\rho}_j^{\mathrm{H}}=\{\rho_j^{\mathrm{H}}(u,v)\}^{M\times N}$ in HILL [Li, Wang, Huang et al. (2014)] using Eq. (3).

$$\boldsymbol{\rho}_j^{\mathrm{H}}=\frac{1}{\left|\mathbf{R}_j\right|\otimes\mathbf{F}_{l1}}\otimes\mathbf{F}_{l2} \tag{3}$$

where $|\cdot|$ represents the absolute value operation, and $\mathbf{F}_{l1}$ and $\mathbf{F}_{l2}$ are average filters sized 3×3 and 15×15 respectively.

Denote the color value distortion caused by modifying $x_j(u,v)$ into $x_j(u,v)+1$ as $\delta_j(u,v)$, as shown in Eq. (4). Where $R_j(u,v)$, $G_j(u,v)$, $B_j(u,v)$, and $R_j^+(u,v)$, $G_j^+(u,v)$, $B_j^+(u,v)$ are the corresponding RGB color values of $x_j(u,v)$ and $x_j(u,v)+1$ respectively.

$$\delta_j(u,v) = [R_j(u,v) - R_j^+(u,v)]^2 + [G_j(u,v) - G_j^+(u,v)_i]^2 + [B_j(u,v) - B_j^+(u,v)]^2 \tag{4}$$

Thus, the texture cost $\rho_j^{\mathrm{T}}(u,v)$ for each $x_j(u,v)$ is defined in Eq. (5). Where the cost $\rho_j^{\mathrm{H}}(u,v)$ is calculate using Eq. (3), which is the same with the cost in HILL.

$$\rho_j^{\mathrm{T}}(u,v) = \delta_j(u,v) \cdot \rho_j^{\mathrm{H}}(u,v) \tag{5}$$

To extract the content profile of frame $\mathbf{X}_j$, it is transformed into grayscale image firstly by replacing $x_j(u,v)$ with the corresponding real luminance value. Then the obtained grayscale image is further transformed into binary image $\mathbf{Y}_j=\{y_j(u,v)\}^{M\times N}$. Thus, the value of the elements in $\mathbf{Y}_j$ are 0 or 1. The content profile of $\mathbf{X}_j$ is the locations corresponding to "0" in $\mathbf{Y}_j$.

The locations corresponding to "1" in $\mathbf{Y}_j$ belong to the background of $\mathbf{X}_j$, which are so smooth that any modifications would be discovered. Therefore, these locations are not suitable for steganography. Accordingly, the profile cost $\boldsymbol{\rho}_j^{\mathrm{P}}=\{\rho_j^{\mathrm{P}}(u,v)\}^{M\times N}$ for each $x_j(u,v)$ can be obtained using Eq. (6).

$$\rho_j^{\mathrm{P}}(u,v) = \begin{cases} 1 & , \quad y_j(u,v) = 0 \\ \infty & , \quad y_j(u,v) = 1 \end{cases} \tag{6}$$

In order to utilize the inter-frame correlation among different $\mathbf{X}_j$, we consider the color difference between $\mathbf{X}_j$ and $\mathbf{X}_{j-1}$. Both $\mathbf{X}_j$ and $\mathbf{X}_{j-1}$ are transformed into grayscale image to calculate the color difference. To avoid the subscript of $\mathbf{X}_j$ overflowing, the embedding tasks are not done on the first frame $\mathbf{X}_1$. That means the first frame is kept unchanged during data embedding. Denote the (u,v)th pixels of the grayscale $\mathbf{X}_j$ and $\mathbf{X}_{j-1}$ as $p_j(u,v)$ and $p_{j-1}(u,v)$ respectively, the color difference $\mathbf{D}_j=\{d_j(u,v)\}$ between $\mathbf{X}_j$ and $\mathbf{X}_{j-1}$ is,

$$d_j(u,v) = \left| p_j(u,v) - p_{j-1}(u,v) \right| \tag{7}$$

Then the variation cost $\boldsymbol{\rho}_j^{\mathrm{V}}=\{\rho_j^{\mathrm{V}}(u,v)\}^{M\times N}$ for each $x_j(u,v)$ is defined in Eq. (8) to decrease the modifications on the frame which is similar with the previous frame.

$$\rho_j^{\mathrm{V}}(u,v) = \begin{cases} 1.3 & , \quad d_j(u,v) < 15 \\ 1 & , \quad d_j(u,v) \geq 15 \end{cases} \tag{8}$$

where the values "1.3" and "15" are empirically determined by experiments.

Finally, the three parts (texture cost $\rho_j^{\mathrm{T}}(u,v)$, profile cost $\rho_j^{\mathrm{P}}(u,v)$, variation cost $\rho_j^{\mathrm{V}}(u,v)$) are combined together by multiplication. The final embedding cost $\rho_j(u,v)$ assigned for $x_j(u,v)$ is defined in Eq. (9).

$$\rho_j(u,v) = \rho_j^{\mathrm{T}}(u,v) \cdot \rho_j^{\mathrm{P}}(u,v) \cdot \rho_j^{\mathrm{V}}(u,v) \tag{9}$$

3 Experimental results

Several experiments are conducted to verify the effectiveness of the proposed distortion function method. Firstly, we setup the experimental environments. Subsequently, we

analyze the quality of stego image. Finally, we provide the results of undetectability compared with HILL.

3.1 Experimental setup

To build the cover image set, we collected 560 emoji images that is widely used in social networks. These images are in palette format and each image contains 256 colors and several frames. There are 2557 frames in total of the 560 images. We have uploaded all the 560 images on https://pan.baidu.com/s/1nOsn_eoI8vLpgqo8ue8nOQ.

We compare the proposed distortion function with the popular distortion function HILL which performs the state-of-the-art undetectability. Since HILL is designed for spatial image, each frame is transformed into grayscale image firstly when embedding with HILL. In other words, for HILL embedding, there are 2557 grayscale images are used as covers. The capacity of secret data embedded in each frame is set as 600 bits, 700 bits, 800 bits, 900 bits, 1000 bits, and 1100 bits respectively. All embedding tasks are done by the embedding simulator [Pevný, Filler and Bas (2010)] since it is widely used to simulate the optimal embedding. For steganalysis, the feature sets SPAM proposed by Pevný et al. [Pevný, Bas and Fridrich (2010)] and SRMQ1 proposed by Fridrich et al. [Fridrich and Kodovsky (2012)] are employed in our experiments. The ensemble classifier proposed by Kodovsky e al. [Kodovsky, Fridrich and Holub (2012)] is used to measure the property of feature sets. In detail, half of the cover and stego feature sets are used as the training set while the remaining half are used as testing set. The criterion to evaluate the performance of feature sets is the minimal total error P_{E} under equal priors achieved on the testing set in Kodovsky et al. [Kodovsky, Fridrich and Holub (2012)]:

$$P_E = \min_{P_{FA}}\left(\frac{P_{\mathrm{FA}} + P_{MD}}{2}\right) \tag{10}$$

where P_{FA} is the false alarm rate and P_{MD} is the missed detection rate. The performance is evaluated using the average value of P_{E} over ten random tests.

3.2 Image quality demonstrations

The demonstrations of the proposed method are shown in Fig. 4. Where Fig. 4(a) is a cover emoji image composed of several frames. After each frame is embedded with 600, 800, and 1000 bits respectively, the obtained stego images are shown in Figs. 4(b), 4(c) and 4(d) correspondingly.

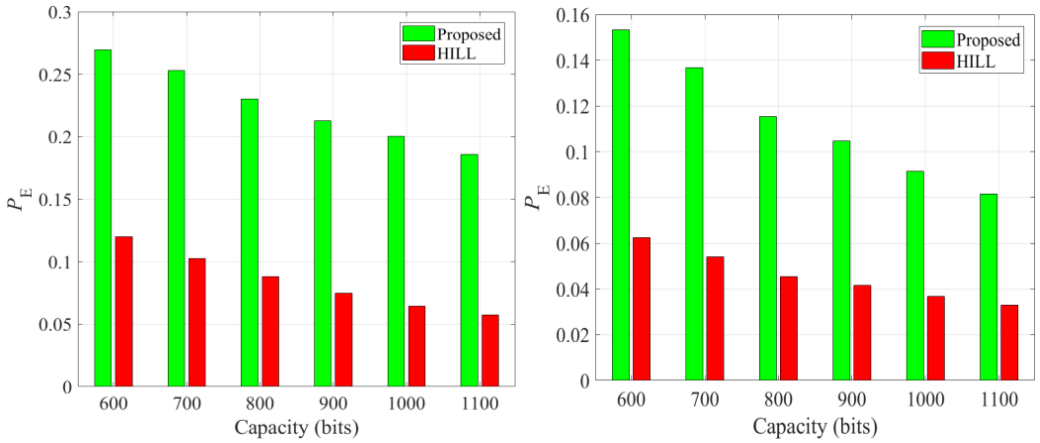
It is clear that the stego images are close to the cover image, which means the visual quality of the stego images is satisfactory regardless of the capacity. Thus, the usability of emoji images is reserved after embedded adequate secret data using the proposed method.

(a) (b) (c) (d)

Figure 4: Demonstrations of (a) cover and corresponding stego emoji images using the proposed method with capacity (b) 600 bits, (c) 800 bits, (d) 1000 bits

3.3 Undetectability comparison

Fig. 5 shows the undetectability comparisons of HILL and the proposed method against SPAM and SRMQ1 tested on all the 2557 frames, and Tab. 1 depicts all numerical values.



(a) (b)

Figure 5: Comparisons of the proposed method with HILL against (a) SPAM, (b) SRMQ1

Table 1: Testing errors of the proposed method and HILL against SPAM and SRMQ1

Steganography Algorithm	Feature	Capacity (bits)					
		600	700	800	900	1000	1100
Proposed	SPAM	0.2696	0.2529	0.2300	0.2127	0.2005	0.1859
	SRMQ1	0.1533	0.1367	0.1153	0.1046	0.0914	0.0815
HILL	SPAM	0.1199	0.1027	0.0879	0.0746	0.0644	0.0574
	SRMQ1	0.0624	0.0540	0.0453	0.0415	0.0368	0.0329

It is clear that the security performance of the proposed method is much better than HILL for all cases, regardless of the steganalytic tools and capacity. Specifically, the P_E values

of the proposed method are more than two times of HILL. For the cases of large capacity, e.g., 900, 1000, 1100 bits, the P_E values of the proposed method are nearly three times of HILL. The large improvement on undetectability is because that the proposed distortion function is designed by following the unique properties of emoji image, while HILL not.

In addition, inter-frame correlation is the most unique property of motion image, which is mentioned in Usui et al. [Usui, Takano and Yamamoto (2017)]. The modifications of steganography should avoid destroying the correlation as far as possible. The correlation can be reflected in the difference between image frames. For this reason, we also give the undetectability comparisons on difference image in Fig. 6 to further demonstrate the superiority of the proposed method. Tab. 2 lists the corresponding numerical values.

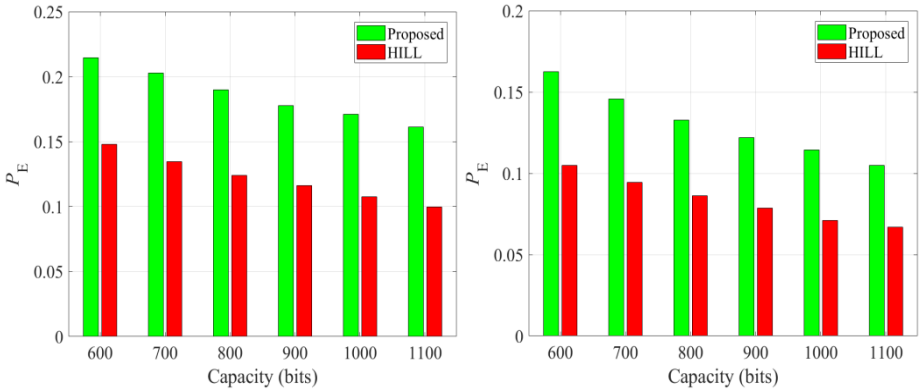


Figure 6: Comparisons on difference image against (a) SPAM, (b) SRMQ1

Table 2: Testing errors tested on difference image against SPAM and SRMQ1

Steganography Algorithm	Feature	Capacity (bits)					
		600	700	800	900	1000	1100
Proposed	SPAM	0.2145	0.2029	0.1898	0.1778	0.1709	0.1613
	SRMQ1	0.1626	0.1457	0.1329	0.1220	0.1144	0.1050
HILL	SPAM	0.1480	0.1346	0.1239	0.1160	0.1075	0.0997
	SRMQ1	0.1050	0.0945	0.0861	0.0787	0.0709	0.0669

Since the first frame is kept unchanged during data embedding, as mentioned in Subsection 2.2, the difference images are obtained by calculating the differences between the first frame and the other frames respectively in each emoji cover and stego image. That means the first frame is kept unchanged during embedding. As shown in Fig. 6, the undetectability

tested on the difference images of the proposed method is still better than HILL.

4 Conclusion

A distortion function for emoji image steganography is proposed in this paper. To fit the properties of emoji image, the profile of image content, the intra- and inter-frame correlation are considered in the proposed distortion function. The three parts are combined together by multiplication to resist steganalysis. Experimental results proved the effectiveness of the proposed distortion function. For further study, it is significant to develop the theoretical optimal embedding for emoji image by uniting the steganographic methods for palette image.

Acknowledgement: This work was supported by the Natural Science Foundation of China (U1736213, 61572308), the Natural Science Foundation of Shanghai (18ZR1427500), the Shanghai Dawn Scholar Plan (14SG36), and the Shanghai Excellent Academic Leader Plan (16XD1401200).

References

Dong, S.; Zhang, R.; Liu, J. (2018): Invisible steganography via generative adversarial network. *Multimedia Tools and Applications*.

Du, Y.; Yin, Z.; Zhang, X. (2018): Improved lossless data hiding for JPEG images based on histogram modification, *Computers, Materials & Continua*, vol. 55, no. 3, pp. 495-507.

Filler, T.; Judas, J.; Fridrich, J. (2011): Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920-935.

Fridrich, J.; Filler, T. (2007): Practical methods for minimizing embedding impact in steganography. *Electronic Imaging*.

Fridrich, J.; Kodovsky, J. (2012): Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868-882.

Fridrich, J.; Soukal, D. (2006): Matrix embedding for large payloads. *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 3, pp. 390-395.

Guan, Z.; Zhang, Y.; Wu, L.; Wu, J.; Ma, Y. et al. (2018): Appa: an anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *Journal of Network and Computer Applications*.

Guo, L.; Ni, J.; Shi, Y. Q. (2014): Uniform embedding for efficient jpeg steganography. *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 5, pp. 814-825.

Guo, L.; Ni, J.; Su, W.; Tang, C.; Shi, Y. Q. (2015): Using statistical image model for jpeg steganography: uniform embedding revisited. *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 12, pp. 2669-2680.

Holub, V.; Fridrich, J. (2012): Designing steganographic distortion using directional filters. *IEEE International Workshop on Information Forensics & Security*.

Holub, V.; Fridrich, J.; Denemark, T. (2014): Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*, vol. 1, no. 1, pp. 1.

Kodovsky, J.; Fridrich, J.; Holub, V. (2012): Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432-444.

Li, B.; Wang, M.; Huang, J.; Li, X. (2015): A new cost function for spatial image steganography. *IEEE International Conference on Image Processing*.

Li, S.; Zhang, X. (2018): Towards construction based data hiding: from secrets to fingerprint images. *IEEE Transactions on Image Processing*, vol. 1, no. 1, pp. 99.

Pevný, T.; Bas, P.; Fridrich, J. (2010): Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215-224.

Pevný, T.; Filler, T.; Bas, P. (2010): Using high-dimensional image models to perform highly undetectable steganography. *Lecture Notes in Computer Science*, vol. 6387, pp. 161-177.

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*.

Qian, Z.; Zhang, X. (2016): Reversible data hiding in encrypted images with distributed source encoding. *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 26, no. 4, pp. 636-646.

Qian, Z.; Zhang, X.; Wang, S. (2014): Reversible data hiding in encrypted JPEG bitstream. *IEEE Transactions on Multimedia*, vol. 16, no. 5, pp. 1486-1491.

Qian, Z.; Zhou, H.; Zhang, X.; Zhang, W. (2016): Separable reversible data hiding in encrypted jpeg bitstreams. *IEEE Transactions on Dependable & Secure Computing*, vol. 15, no. 6, pp. 1055-1067.

Sedighi, V.; Cogranne, R.; Fridrich, J. (2015): Content-adaptive steganography by minimizing statistical detectability. *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221-234.

Tzeng, C; Yang, Z.; Tsai, W. (2004): Adaptive data hiding in palette images by color ordering and mapping with security protection. *IEEE Transactions on Communications,* vol. 52, no. 5, pp. 791-800.

Usui, T.; Takano, Y.; Yamamoto, T. (2017): A study on a driving method of OLED displays for better motion image quality with adaptive temporal aperture control: a lifetime and motion image quality for OLEDs. *Journal of the Society for Information Display*.

Wang, Z; Qian, Z.; Zhang, X.; Yang, M.; Ye, D. (2018): On improving distortion functions for JPEG steganography. *IEEE Access*, vol. 6, no. 1, pp. 74917-74930.

Wang, Z.; Yin, Z.; Zhang, X. (2019): Asymmetric distortion function for JPEG steganography using block artifact compensation. *International Journal of Digital Crime and Forensics*, vol. 11, no. 1, pp. 90-99.

Wang, Z.; Yin, Z.; Zhang, X. (2017): Distortion function for jpeg steganography based on image texture and correlation in dct domain. *IETE Technical Review*, vol. 35, no. 4, pp.

351-358.

Wang, Z.; Zhang, X.; Yin, Z. (2016): Hybrid distortion function for JPEG steganography. *Journal of Electronic Imaging*, vol. 25, no. 5, 050501.

Wang, Z.; Zhang, X.; Yin, Z. (2018): Joint cover-selection and payload-allocation by steganographic distortion optimization. *IEEE Signal Processing Letters*, vol. 25, no. 10, pp. 1530-1534.

Wei, Q.; Yin, Z.; Wang, Z.; Zhang, X. (2017): Distortion function based on residual blocks for JPEG steganography. *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 17875-17888.

Wu, J.; Dong, M.; Ota, K.; Li, J.; Guan, Z. (2018): Big data analysis-based secure cluster management for optimized control plane in software-defined networks. *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 27-38.

Zhang, W.; Zhang, X.; Wang, S. (2008): Maximizing steganographic embedding efficiency by combining hamming codes and wet paper codes. *Information Hiding, Lecture Notes in Computer Science*, vol. 5284, pp. 60-71.

Zhang, X.; Wang, S. (2006): Efficient steganographic embedding by exploiting modification direction. *Communications Letters IEEE*, vol. 10, no. 11, pp. 781-783.