Data Hiding in Iris Image for Privacy Protection

Sheng Li, Xin Chen, Zichi Wang, Zhenxing Qian and Xinpeng Zhang
Shanghai Institute for Advanced Communication and Data Science, School of Communication & Information Engineering, Shanghai University, Shanghai, People’s Republic of China

ABSTRACT
This paper proposes a novel iris image data hiding scheme for privacy protection. Privacy personal data is embedded into the iris image such that its impact on the iris recognition is minimised. This is achieved by restricting the modifications of the embedding within the regions that seldom affects the iris recognition with the help of the STC (syndrome trellis coding) framework. We also propose a novel distortion function to measure the impact of the data embedding on iris recognition, where the regions with important iris features are assigned with high embedding cost. Experimental results show that, by using our proposed scheme, we can embed sufficient data into the iris image with high recognition accuracy maintained.

KEYWORDS
Data hiding; Distortion function; Iris image; Privacy protection

1. INTRODUCTION

Traditional authentication methods are mainly based on tokens e.g. ID cards, or knowledge, e.g. passwords [1]. The former is easy to lost and copied, and the latter is at risk of being forgotten or stolen. Because of this, biometric authentication technology has been widely developed recently [2]. According to the origin, bio-characteristics can be divided into physiological bio-characteristics, e.g. fingerprints, irises, faces, DNA, etc. and behavioural bio-characteristics, e.g. signatures, voiceprints, gait, etc. These biometric characteristics are generally unique, life-immutable, and hard to be forgotten or stolen during identity authentication.

Among the various biometric authentication systems, iris authentication [3] has attracted great attention due to its stable recognition performance and high recognition rate. In the existing iris authentication systems, personal iris images are collected as biometric templates by an authorising institution and stored in different types of sub-databases with the corresponding personal privacy data, e.g. name, phone number, address, bank account, etc. The personal privacy data stored separately in a database also has a great risk of theft. Therefore, how to protect these personal privacy data while minimising the iris recognition accuracy has become a serious issue.

Data hiding [4,5] is one of the main techniques for privacy protection. The aim of biometric data hiding [6–13] is to embed sufficient personal data into cover biometric templates and to maintain the performance of recognition. Existing biometric data hiding methods usually perform the data embedding on the region that does not contain key features of the biometrics. For example, Vatsa et al. [9] use phase consistency to detect the location of human face features, data is embedded into the rest locations. Whitelam et al. [11] use multi-layer watermarking and steganography to protect multi-modal biometric information. In [12], the iris template data is embedded only in the blue channel. Though these schemes achieve reasonably good performance for biometric image data hiding. How to minimise the impact of the data embedding on the biometrics recognition remains unanswered.

In this paper, we incorporate the STC [14] framework for iris image data hiding, where the impact of the data embedding on the iris recognition is minimised. Concretely, the personal privacy data is embedded in an iris image using STC with a proposed distortion function, which assigns high embedding costs for the regions to contain important iris features for recognition. During the data embedding, the modifications are restricted into the regions with minimised iris recognition impact. Experimental results show that we are able to embed sufficient personal data into the iris image while maintaining a high-recognition accuracy.

The rest of this paper is organised as follows. We introduce the related works in Section 2. The proposed method described in Section 3. Experimental results and analysis are provided in Section 4. Section 5 concludes the whole paper.
2. RELATED WORKS

In this Section, some related works are introduced, including watermarking and steganography-based biometric data protection methods.

Jain et al. [8] proposed two scenarios for biometric data protection. In the first scenario, the fingerprint minutiae data is hidden in a cover image to protect the fingerprint minutiae before the image is transmitted through a public channel. In the other scenario, face information is embedded into a fingerprint image as watermarking and then registered on a smart card. At the phase of authentication, the fingerprint image and the reconstructed face image can be extracted for multi-factor authentication. In [9], Vatsa et al. proposed a 3-layer RDWT bio-watermarking algorithm to embed biometric Mel Frequency Cepstral Coefficients (MFCC) coefficients into colour face images. In this way, the robustness and safety of system are enhanced. It firstly uses phase consistency to detect the location of human face features. Furthermore, these key feature areas in the watermark algorithm are skipped, so that the accuracy of the face recognition system is slightly affected.

Li et al. [10] propose a new scheme for protecting biometric templates using a saliency region’s authentication watermarking. A multi-level authentication watermarking scheme is firstly proposed to verify the integrity of biometrics. Secondly, principal component analysis (PCA) features of these biometric images are used as watermarks to recover tampered images. Based on the detection result of the salient region, the authentication bits and the information bits can be adaptively embedded in the biometric image. Whitelam et al. [11] proposed a framework that uses multi-layer watermarking and steganography to protect multi-modal biometric information. The specific approach is to use the watermark technology specifically for grayscale images to embed human face features into corresponding fingerprint images. The watermark image is then embedded in any cover image that is not related to biometrics. If the cover is attacked, this method does not show any possibility of the existence of biometric data, which can provide the user with an extra layer of security.

Chaudhary et al. [12] propose an LSB-based steganographic method to protect colour iris template. In order to enhance security, the iris template data is embedded only in the blue channel. In the authentication system, the cover image embedded with the iris template can be directly stored to avoid storing the original biometric data of privacy. Li et al. [7] proposed a privacy fingerprint authentication system. Personal privacy data is embedded into binary template fingerprint images. Since no boundary pixels are generated during the embedding process, the distortion caused to the cover can be minimised. The embedding method causes the smallest possible anomaly in the refinement of the fingerprint template without affecting the recognition performance of the fingerprint authentication system. A template protection and fusion strategy are proposed in [13]. Fingerprint feature vectors and iris features are used as watermarks. The watermark is then embedded in the low-frequency AC coefficient of the smooth 8×8 DCT block in the image. Decision-level fusion strategy is used to improve the overall performance of multi-modal systems. Tarif et al. [6] proposed a method for ensuring the secure transmission of biometric data by means of encryption and information hiding in a multi-modal authentication biometric system. The fingerprint and iris biometric template are embedded into the Slantlet-SVD transform domain of the face image.

In this paper, we propose a data hiding method for the privacy protection of iris image using STC embedding with a proposed distortion function. To the best of our knowledge, we are unable to find any literature which takes advantage of the STC framework for biometrics data hiding.

3. THE PROPOSED METHOD

In this paper, a data hiding method for iris image is proposed. The personal privacy data is embedded in an iris image using STC-based data hiding. To minimises the impact of data embedding on the iris recognition, we propose a novel distortion function by assigning high embedding cost for the region with important iris features.

3.1 The System

Figure 1 shows the iris authentication system considered in this paper. In enrolment phase, the personal privacy data M is firstly encrypted into cipher text M′ using existing encryption algorithms, e.g. data encryption standard (DES), international data encryption algorithm (IDEA) with an embedding key K. Then M′ is embedded into a registered iris image C using a proposed embedding algorithm to obtain the iris image S with secret data. Finally, S is stored in the iris database for authentication. In this phase, only one iris image database is needed, instead of additional storage space.
In the authentication phase, an iris image is processed to obtain its iris code $T_i$. Then another iris code $T_j$ is extracted from the iris image in the database, and then used for verification by matching. The matching is passed when the matching score is higher than the threshold $\tau$ set by the system. The cipher text $M'$ can be extracted from the iris image in the database when the matching is passed. After decryption with the same key $K$, the personal privacy data $M$ is obtained and returned to the user. If the matching is failed, the privacy data will not be extracted.

### 3.2 STC-based Data Embedding and Extraction

In the proposed method, the STC framework is employed for data embedding. Denote the size of a cover image as $k \times l$, the $(i, j)$th element as $c(i, j)$, and the embedding cost assigned for $c(i, j)$ as $\rho(i, j)$, where $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, l$. The theoretical minimal steganography distortion $D$ of stego image with embedding capacity $m$ (bits) [15] is,

$$D = \sum_{i=1}^{k} \sum_{j=1}^{l} p(i, j) \rho(i, j)$$

where

$$p(i, j) = \frac{e^{-\lambda \rho(i, j)}}{1 + e^{-\lambda \rho(i, j)}}$$

are the probabilities of modifying $c(i, j)$. The parameter $\lambda$ ($\lambda > 0$) is used to make the information entropy of modification probability equal to the capacity $m$,

$$- \sum_{i=1}^{k} \sum_{j=1}^{l} [p(i, j) \log_2 p(i, j) + (1 - p(i, j))] \log_2 [1 - p(i, j)] = m$$

The STC coding provides a practical encoding scheme to approach this theoretical bound. Once the embedding costs are specified, the secret data can be embedded into the cover by STC.

In the phase of data embedding, the elements of a cover image, the distortion function, and secret data are inputted into STC (with a constraint height $h = 10$) to generate the output stego. Let secret data be $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_m]^T \in \{0,1\}^m$. Then, $\alpha$ can be embedded into
In the phase of data extraction, the secret data stego elements $\alpha = \text{computation},$ adaptively, where $s = [s_1, s_2, \ldots, s_k] \top$ is the elements of stego image, and $C(\alpha)$ is the coset of $\alpha$.

In the phase of data extraction, the secret data $\alpha$ in the stego elements $s$ can be directly extracted by a matrix computation,

$$\alpha = Hs$$

where $H$ is a low-density parity-check matrix that is pre-defined determined by the embedding speed, the embedding efficiency and the payload.

Therefore, the distortion function is the most crucial factor in STC-based data embedding framework. There are many distortion functions, e.g. HUGO [16], WOW [17], S-UNIWARD [18], HILL [19], etc. These distortion functions aim to embed the secret into complex areas as much as possible. Such operations on iris images may destroy its features, which leads to the reduction of the recognition performance of the iris authentication system. For this reason, in the next subsection, we designed a novel distortion function for the iris image.

### 3.3 The Distortion Function

To minimise the impact on the iris recognition caused by embedding, a new distortion function is proposed. Since the edge area of the iris image contains no key iris features, the accuracy of the iris recognition system is seldom affected by data embedding in the edge area. This motivates us to incorporate the edge detection for the design of the distortion function. Any edge detection algorithm can be adopted for this purpose. In our implementation, we adopt the canny edge detector which is a classic and fast edge detection algorithm.

There are two main steps for the design of the distortion function. Firstly, the canny edge detection algorithm [20] is employed to produce an initial embedding cost for each image element. Then the gradient of the image is exploited to adjust the embedding cost.

As shown in Algorithm 1, the dichotomy method is used to determine the threshold $t_h$ of canny edge detection adaptively, where $q$ is a factor to adjust the range of edge which is set as 0.02 in experiments.

After the threshold of canny detection $t_h$ is obtained, the canny edge detection algorithm is performed on the cover image to find the edge positions. The embedding costs of other non-edge positions are set to infinite to avoid these smooth positions been modified. This is because that the modifications on smooth positions would decrease image quality seriously. The embedding costs of the edge positions are calculated as follows.

Firstly, the gradient values of the cover image are calculated, which can reflect the changing magnitude in various directions. Denote the gradient of $c(i, j)$ in the horizontal direction as $G_x(i, j)$, in the vertical direction as $G_y(i, j)$. As shown in Figure 2, the three-neighbor average absolute values $G_y(i, j)$ and $G_y(i, j)$ of gradient for $c(i, j)$ in horizontal and vertical directions are calculated respectively using Equation (6) and (7). In natural images, the spatial correlation in horizontal and vertical direction is significantly stronger than diagonal direction. For saving the computational complexity, we use only the horizontal and vertical direction to calculate the gradient values.

$$G_h(i, j) = \frac{1}{3} \left[ |G_x(i, j)| + |G_x(i, j - 1)| + |G_x(i, j + 1)| \right]$$

$$G_v(i, j) = \frac{1}{3} \left[ |G_y(i, j)| + |G_y(i - 1, j)| + |G_y(i + 1, j)| \right]$$

### Algorithm 1 Obtaining threshold for edge detection

```
Set $t_{\min} = 0$, $t_{\max} = 1$, $n = 0$
while $m \leq n \leq (1 + q)m$ is not satisfied,
    $t_h = (t_{\min} + t_{\max})/2$
Set the threshold of the canny edge detection algorithm as $t_h$ to update the numbers of edge pixels $n$
if $n \geq m$, $t_{\min} = t_h$
else $t_{\max} = t_h$
end
```

Figure 2: The neighbouring gradients in (a) horizontal direction and (b) vertical direction

$$G_x(i-1, j-1)$$
$$G_x(i-1, j)$$
$$G_x(i-1, j+1)$$
$$G_x(i, j-1)$$
$$G_x(i, j)$$
$$G_x(i, j+1)$$
$$G_x(i+1, j-1)$$
$$G_x(i+1, j)$$
$$G_x(i+1, j+1)$$

$$G_y(i-1, j-1)$$
$$G_y(i-1, j)$$
$$G_y(i-1, j+1)$$
$$G_y(i, j-1)$$
$$G_y(i, j)$$
$$G_y(i, j+1)$$
$$G_y(i+1, j-1)$$
$$G_y(i+1, j)$$
$$G_y(i+1, j+1)$$
After $G_h(i, j)$ and $G_v(i, j)$ are obtained, which characterise the complexity around $c(i, j)$ in both horizontal and vertical directions, a complexity value $\zeta(i, j)$ of $c(i, j)$ is calculated using Equation (8).

$$\zeta(i, j) = \sqrt{G_h(i, j)^2 + G_v(i, j)^2} \quad (8)$$

A larger $\zeta(i, j)$ means more complex texture, thus the corresponding embedding cost should be smaller since complex locations affect image quality weekly. In other words, the value of embedding cost should in inverse proportion to the value of $\zeta(i, j)$. According to this, the proposed distortion function is defined as,

$$\rho(i, j) = \begin{cases} \frac{\mu}{\zeta(x, y)}, & c(i, j) \in E \text{ and } c(i, j) \neq 0, 255 \\ \infty, & \text{otherwise} \end{cases}$$

(9)

where $\mu$ is a positive number and is set as 6 in experiments, $E$ is the edge positions obtained by canny edge detection algorithm mentioned above. In STC-based data embedding, the value of a pixel may be changed by +1 or −1. In a grayscale iris image, the range of the pixel value is from 0 to 255. To avoid the overflow, we have to suspend all the pixels with the value of 0 and 255. Since the secret data can be correctly extracted by the matrix computation defined in Equation (5), it is unnecessary to suspend other pixels.

The proposed distortion function assigns high embedding costs for the regions with important iris features. Combining with STC, impact on the iris recognition caused by embedding is minimised.

4. EXPERIMENT RESULTS

The CASIA-IrisV2-device1 iris database [21] is used to measure the performance of the iris recognition system. We choose the 60 classes, 10 images for each class, and a total of 600 BMP images sized 640×480 for experimentation.

4.1 Embedding Cost

Figure 3 (a) indicates the embedding costs calculated on an iris image, which is marked with white. The brighter the mark is, the smaller the embedding cost and larger modification possibility represented, and vice versa. The black area is the non-edge area, in which the embedding cost is set infinitely.

Figure 3 (b) shows the iris region obtained by the iris region detection method mentioned above. It can be seen that the modification positions are concentrated at the complex area and not at the iris feature region using the proposed method. Therefore, it minimises the impact on iris recognition performance furthest.

4.2 Recognition Rate

In the authentication, the iris recognition system compares the query iris image with the corresponding iris image in the database to obtain the matching score. The larger the matching score, the larger the probability that the two are from the same individual. We employ the receiver operating characteristic (ROC) curves to measure the performance of iris recognition. The ROC curve is plotted based on the Successful Match Rate (SMR) against the False Accept Rate (FAR). The FAR is the ratio of the matching scores in the false matches that are greater than or equal to the threshold $\tau$ set by the system. The value of $\tau$ is determined by the value of FAR, where

$$\text{FAR} = \frac{|\{|s_{ij} \geq \tau, s'_{ij} \in M\}||}{|M|} \quad (10)$$

where $s_{ij}$ means the matching scores of the first samples of different individuals, $M$ denotes the set of all scores, and $|\cdot|$ denotes the number of internal satisfied conditions. The SMR indicates the ratio of the scores in the genuine matches that are greater than or equal to $\tau$, where

$$\text{SMR} = \frac{|\{|s'_{ij} \geq \tau, s'_{ij} \in N\}||}{|N|} \quad (11)$$

where $s'_{ij}$ means the matching scores of the samples of the same individuals and $N$ denotes their set.

We use a pseudo-random number generator to simulate personal privacy data for embedding. The iris images without personal data are used as the query to match the corresponding images in the database to obtain the matching scores. The proposed method, the STC-based embedding algorithms HILL [19], S-UNIWARD [18], HUGO [16], and the non STC-based embedding algorithms EMD [22] and matrix embedding [23] are used to
embed with payload 0.15 bpp (bit per pixel). The ROC curves are shown in Figure 4. For comparison, the original ROC curve without any embedding operation is also plotted. It can be seen that the proposed method performs a slighter drop of the recognition rate. Comparing with non STC-based embedding algorithms, the STC-based embedding algorithms perform better recognition rate since the image content is taken into account. Furthermore, the proposed method achieves the best recognition rate among all the embedding algorithms since the proposed distortion function is designed with the guidance of recognition rate.

The curve of SMR against the payload is shown in Figure 5 with $\text{FAR} = 10^{-4}$. It can be seen that the proposed method performs better recognition rate for all cases. When the payload is large enough such as 0.2 bpp, the personal data may be embedded into the iris feature region, which would result in the decreasing of iris recognition accuracy. In this case, the advantage of the proposed method becomes not obvious. For this reason, the recognition rates of the several methods are similar when payload is larger than 0.2 bpp.

5. CONCLUSION

This paper proposes a data hiding method for iris image. To minimise the impact on the iris recognition, the embedding modifications are restricted into the regions without important iris features with the help of the proposed distortion function and STC framework. After the personal privacy data is embedded in iris images, the privacy of users is protected. In this way, no additional storage space is needed. Experimental results show that we are able to embed sufficient personal data into the iris image and maintain a high recognition accuracy meanwhile. For further study, we will focus on the data hiding methods of other biometric images.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

FUNDING

This work was supported in part by the National Natural Science Foundation of China under Grants 61602294, U1536108, 61572308, U1636206, 61525203, 61472235, and U1736213, in part by the Shanghai Sailing Program under Grant 16YF1404100, in part by the Young Oriental Scholar under Shanghai Institutions of Higher Education, in part by the Shanghai Dawn Scholar Plan under Grant 14SG36 and in part by the Shanghai Excellent Academic Leader Plan under Grant 16XD1401200.

REFERENCES

1. Handbook of biometrics[M]. New York, NY: Springer Science & Business Media, 2007.

2. A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition[],” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, no. 1, pp. 4–20, 2004.

3. L. Masek. Recognition of Human Iris Patterns for Biometric Identification [D]. The University of Western Australia, 2003.

4. C. Qin, C. C. Chang, and YP. Chiu ,“A novel joint data-hiding and compression scheme based on SMVQ and image inpainting[],” IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, Vol. 23, no. 3, pp. 969–978, 2014.
5. C. Qin, and X. Zhang, “Effective reversible data hiding in encrypted image with privacy protection for image content [J].” *Journal of Visual Communication & Image Representation*, Vol. 31, pp. 154–164, 2015.

6. E. B. Tarif, S. Wibowo, S. Wasimi, et al., “A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system[J],” *Multimed Tools Appl*, Vol. 77, no. 2, pp. 2485–2503, 2018.

7. S. Li, and A. C. Kot, “Privacy protection of fingerprint database[J],” *IEEE Signal Process Lett*, Vol. 18, no. 2, pp. 115–118, 2011.

8. A. K. Jain, and U. Uludag, “Hiding biometric data[J],” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 25, no. 11, pp. 1494–1498, 2003.

9. M. Vatsa, R. Singh, and A. Noore, “Feature based RDWT watermarking for multimodal biometric system[J].” *Image Vis Comput*, Vol. 27, no. 3, pp. 293–304, 2009.

10. L. Li C, B. Ma, Y. Wang, et al., 2010. “Protecting biometric templates using authentication watermarking[C],” Pacific-Rim Conference on Multimedia. Springer, Berlin, Heidelberg, 2010, pp. 709–718.

11. C. Whitelam, N. Osia, T. Bourlai, 2013. “Securing multimodal biometric data through watermarking and steganography[C],” Technologies for Homeland Security (HST), 2013 IEEE International Conference on. IEEE, 2013, pp. 61–66.

12. S. Chaudhary, R. Nath, 2015. “A new template protection approach for iris recognition[C],” Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015 4th International Conference on. IEEE, 2015, pp. 1–6.

13. M. Paunwal, S. Patnaik, “Biometric template protection with DCT-based watermarking[J],” *Machine Vision and Applications*, Vol. 25, no. 1, pp. 263–275, 2014.

14. T. Filler, J. Judas, and J. Fridrich, “Minimizing additive distortion in steganography using syndrome-trellis codes[J],” *IEEE Trans Inf Forensics Secur*, Vol. 6, no. 3, pp. 920–935, 2011.

15. J. Fridrich, and T. Filler, 2007. “Practical methods for minimizing embedding impact in steganography[C],” Security, Steganography, and Watermarking of Multimedia Contents IX. International Society for Optics and Photonics, 2007, Vol. 6505, p. 650502.

16. T. Pevný, T. Filler, and P. Bas, 2010. “Using high-dimensional image models to perform highly undetectable steganography[C],” International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 2010, pp. 161–177.

17. V. Holub, and J. Fridrich, 2012. “Designing steganographic distortion using directional filters[C]//Information Forensics and Security (WIFS), 2012 IEEE International Workshop on. IEEE, 2012, pp. 234–239.

18. V. Holub, and J. Fridrich, 2013. “Digital image steganography using universal distortion[C],” Proceedings of the first ACM workshop on Information hiding and multimedia security. ACM, 2013, pp. 59–68.

19. B. Li, M. Wang, J. Huang, et al., 2014. “A new cost function for spatial image steganography[C],” Image Processing (ICIP), 2014 IEEE International Conference on. IEEE, 2014, pp. 4206–4210.

20. J. Canny, “A computational approach to edge detection[M],” *Readings in Computer Vision*, Vol. 6, pp. 184–203, 1987.

21. http://biometrics.idealtest.org/findTotalDbByMode.do?mode = Iris. Accessed 6 April 2018.

22. X. Zhang, and S. Wang, Efficient steganographic embedding by exploiting modification direction[J]. *IEEE Commun Lett*, Vol. 10, no. 11, pp. 781–783, 2006.

23. J. Fridrich, and D. Soukal, “Matrix embedding for large payloads[J],” *IEEE Trans Inf Forensics Secur*, Vol. 1, no. 3, pp. 390–395, 2006.
Authors

Sheng Li received the PhD degree at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2013. From 2013 to 2016, he was a research fellow in Rapid Rich Object Search (ROSE) Lab, Nanyang Technological University. He is currently with the faculty of the School of Communication and Information Engineering, Shanghai University, China. His research interests include biometric template protection, pattern recognition, multimedia forensics and security. He is the recipient of the IEEE WIFS Best Student Paper Silver Award.

E-mail: shengli@shu.edu.cn.

Xin Chen received the BS degree at Donghua University, Shanghai, China. In 2016. He is now pursuing the MS Degree at the School of Communication and Information Engineering, Shanghai University, China. His research interests include biometric privacy protection and biometric data hiding.

E-mail: shuchenxin@shu.edu.cn.

Zichen Wang received the BS degree in electronics and information engineering from Shanghai University, China, in 2014, and the MS degree in signal and information processing from the same university in 2017. He is currently pursuing the PhD degree at Shanghai University, China. His research interests include steganography, steganalysis and reversible data hiding. He has published about 10 papers in these areas.

Corresponding author. E-mail: wangzichi@shu.edu.cn.

Zhenxing Qian received both the BS and the PhD degrees from University of Science and Technology of China (USTC) in 2003 and 2007, respectively. Since 2009, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a Professor. His research interests include information hiding and multimedia security.

E-mail: zxqian@shu.edu.cn.

Xinpeng Zhang received the BS degree in computational mathematics from Jilin University, China, in 1995, and the ME and PhD degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a professor. His research interests include information hiding, image processing, and digital forensics. He has published over 200 papers in these areas.

E-mail: xzhang@shu.edu.cn.