SIFT特徴値の可逆回転による電子透かし手法

黄　緒平[1,a)]

概要：本論文は医療データの機密性を保証するため，スケール不変特徴変換（SIFT）特徴値への可逆回転に基づいた電子透かし埋め込み場所の特定手法を提案する．回転係数は三角行列に分解し，特徴値の座標に角度パラメータによる可逆な回転を適応する．スケールのヒストグラム及び劣化の期待値を用い，回転された位置に埋め込みを行う．抽出は逆回転より実現する．平均ステゴデータ生成の計算時間 0.397s，ピーク信号対雑音比 50.595 dB 及びエントロピー 5.216 の評価結果により，本手法の有効性を示した．

キーワード：電子透かし，スケール不変特徴変換，可逆回転，機密性

Watermarking Location Specification Method by SIFT Feature Reversible Rotation

Xuping HUANG[1,a)]

Abstract: This paper proposes a new watermarking technique based on scale invariant feature transform (SIFT) integer rotation to protect the confidentiality of medical data. SIFT is used to extract the positions of the original data, and then the positions are rotated by a reversible integer rotation algorithm by multiplying triangular matrix to generate the appropriate positions for embedding an encrypted and divided person data of patients. Histogram of scale and distortion is estimated to generate the stego data. Different positions according histogram of scale are used for embedding after applying integer rotation with angles as an alternative parameter. The experimental results show the proposed watermarking method imperceptible with an average peak signal-to-noise ratio (PSNR [dB]) 50.595 and 5.216 as the average entropy.

Keywords: Watermarking, Integer Rotation, SIFT, Data Confidentiality

1. Introduction

1.1 Purpose statement

Recently, the highly development of ICT, the remote online medical clinic has supply an alternative solution for health-care. Machine learning and artificial intelligence technologies promises bright future for computer-aided medical diagnosis. In this scenario, digital personal data, including sensitive personal information and electronic medical chart, may be shared among different hospitals and research institutes. Furthermore, spoofing and abuse of biometric authentication may be a serious social problem. A wrist Nymi band can use electrocardiography biometrics for authentication to unlock and login ubiquitous devices, including cars, PCs and even personal online bank account, etc. It also pointed out the security risky of disclosure of waveform of heart rate to the untrusted third party, since a generated waveform after training with piece of biometrics data can successfully attack the authentication system of IoT [1]. The confidentiality of personal data, including medical image and personal sensitive data, should be considered as an important issue and the private medical data should be protected in the case of multiple data providers for a secure medical information disclosure [2],[3].

[1] 公立大学法人首都大学東京　産業技術大学院大学
Advanced Institute of Industrial Technology
[a)] huang-xuping@aiit.ac.jp

1.2 Conventional works

In order to guarantee the confidentiality of privacy data of patients to supply a secure data sharing system for medical data. The following technologies are focused. (1) *Secure Computing:* Encrypted statistics for distributed data are proposed [3][4][5], which is also called privacy-preserving data mining (PPDM), e.g. logistic regression, linear regression by homonmorphic encryption. High computing performance is necessary, since homomorphic encryption generate a huge amount of data by key with a length of 1024 bits; (2) *Data Anonymization:* This solution is to protect data by removing personally identifier information by suppression or generalization using *k-anonymity, l-diversity, t-closeness* methods [6]. The disadvantage is irreversible data loss for anonymization process; (3) *Differential Privacy:* The mechanism is to add noise to the raw data with sensibility. The mechanism of noise generation consider security utility and usability, which is corresponding to queries or operations [7][8][9]; and (4) *Watermarking and steganography:* Data required confidentiality are embedded into another innocent cover data, and it is available to the trust users after extraction via data transmit channel [10][11].

1.3 Novelty and contribution of this work

This paper focuses on watermarked approach to protect sensitive patients personal data during the medical information disclosure. The scenario is to hide personal information into the medical image in the set of electronic medical record as the payload, including personal information, medicine history, etc. The distortion of medical image is controlled to be imperceptible, to make the information comprehensive. This approach aims to get the best balance between data disclosure and data confidentiality, in the case of online clinic, and medical data sharing in several parties as the target application.

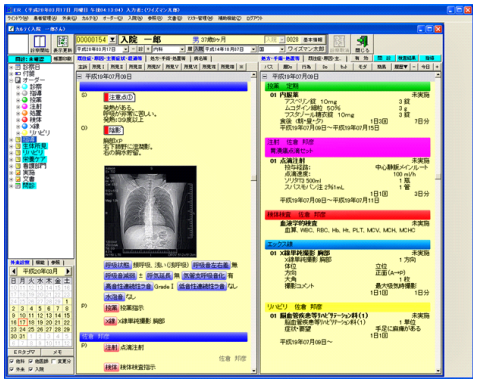


図 1 An example of electronic medical record in Japan.

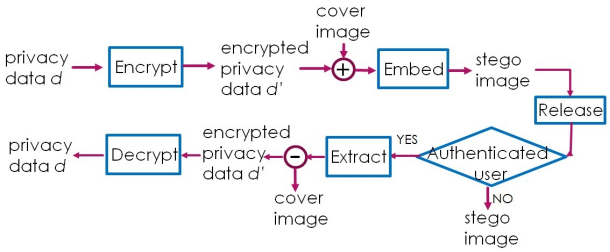


図 2 Scenario of the proposed method (1): protect the privacy of electronic medical record

Figure 1 shows an example of electronic medical record in Japan. Personal data is disclosed with text and image information. For the future usage of the proposed work, there are two target applications with the purpose of (1) guarantee the sensitive data of person data for patients, as plotted in Fig. 2; and (2) tampering detection of electronic medical record, as plotted in Fig. 3. Since the purpose of usage (1) is to assure the confidentiality of the privacy data, encryption is applied and then embedded into image data, which is a double assurance. The the key is shared between the authenticated users to decrypt the privacy data. Being different from (1), the purpose of user (2) is to detect whether the information of the electrical medical record has been tampered, the payload will be generated by hash function, and then embedded into original data for verification. The trusted users, including researchers or doctors may extract the data by the shared watermark key, including extraction algorithm, positions to generate the reconstructed original data, and the extracted payload. The extracted payload is used to compared to those hash values generated by the reconstructed original data. For both of the usages, the common part is the embedding algorithm, since for both of application, distortion of original data should be assured. We explore the hiding algorithm to find proper positions for hiding, and to evaluate the distortion coursed by embedding. The main focus is to explore the appreciate embedding positions based on a reversible rotation algorithm applying to SIFT keypoints. Implementation are based on replacement to evaluate the effectiveness of the proposed method towards distortion, with proper hiding capacity. However, the data loss occurs, and there are more alternative methods here to hide information, we mainly focus on the adequateness of the hiding positions as the preliminary work. We will develop more robust algorithm for embedding in the future, including applying integer discrete cosine transform to the image points, using the mechanism of reserving embedding positions proposed in this paper.

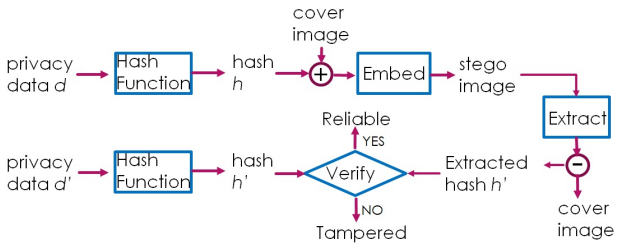


図 3 Scenario of the proposed method (2): tampering detection of electronic medical record

The most effective watermarking methods with high capacity and quality are based on hiding information in both of the time domain and the frequency domain. Payload is embedded to discrete cosine transform (DCT) coefficients [12][13], embedding upon residue after linear predictive coding (LPC) after expansion [14] by multiplication, and in selected SIFT positions, etc. Low, middle and high DCT coefficients are selected for robustness and imperceptibility purposes. Watermarking based on SIFT is also a popular approach [15][16][17][18]. In these approaches, the SIFT feature points are used to determine the hiding positions. In work [15], the marked regions were selected around the SIFT feature points then normalized to a uniform size against scaling attack, and watermarks were embedded into these normalized regions. Even though the advantage of SIFT against geometric attacks, there is a disadvantage in SIFT-based watermarking that the redetection ratio of SIFT feature points declines after watermarks are embedded into regions including SIFT feature points. To avoid negative influence of embedding watermarks, a watermarking method embedding surrounding regions of SIFT feature points was proposed in work [16]. However, the feature points surrounding is vulnerable since the complexity to estimate the hiding positions is $log(n)$. In this work, we also focus on SIFT-based watermarking, since the SIFT-based watermarking are verified to be robust against conventional attacks and geometric attacks, especially in terms of rotation, translation and clipping [17][18].

In this work, the embedding positions are selected after applying a reversible and integer rotation algorithm to SIFT feature points. The positions integer rotation is a novel propose here since the rotation algorithm include $sin()$ and $cos()$ calculation, with a rotation angle α as the parameter. This position integer rotation makes the embedding positions robust enough against geometric attacks, and keeps a certain of complexity accordingly. Additionally, since it is a reversible algorithm, the original positions can be available if necessary. The hiding positions are kept as a part of key to extract the embedded information from the stego data. Replacement is used for embedding as a preliminary process to show the payload and the imperceptibility of the proposed embedding algorithm, that data in SIFT positions are kept as a part of data to reconstruct the original data. An algorithm to achieve a robust hiding positions with imperceptibility is focused in this paper rather than the hiding algorithm. A reversible embedding mechanism will be enhanced in our future work.

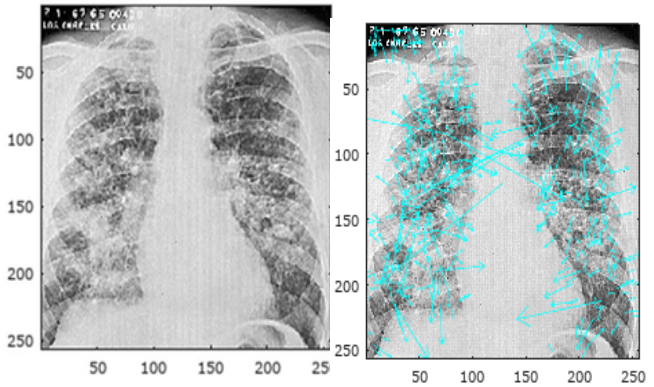
This paper is organized as follows. The approaches is discussed in Section 1. Sections 2 describes the proposed method in detail. Section 3 summarizes the experimental evaluation results. We conclude the paper in Section 4.

2. Proposed method and implementation: watermarking based on SIFT positions integer rotation

In this paper, we propose a geometrical robust SIFT-based watermarking method for healthcare images. Being different from the conventional works, which embed payload data into SIFT feature points, surrounding points and adjacent points, we propose an reversible integer rotation algorithm to determine the hiding positions, which include $sin()$, $cos()$ processing with a angle parameter $\alpha, (0 \leq \alpha \leq 360)$. While the rotation angle is specified to be $-\alpha$, the feature points positions can be relocated successfully, without any location map to restore this information.

2.1 SIFT keypoints detection

Keypoint descriptor is used in SIFT, which is proposed originally in Lowe's works [20][21]. This paper use the



(a). Original image: chest_x-ray.bmp from SIDBA, 256x256, gray (b) Image with SIFT keypoints detected

図 4 An example of medical image: original and with SIFT keypoints.

	position (x, y)		scale	orientation
1	122.29	128.49	22.96	-2.559
2	100.23	126.78	17.56	-2.67
3	84.27	74.94	20.5	2.99
4	84.27	74.94	20.5	-0.428
5	75.42	179.59	21.64	-2.75
6	97.63	126.87	16.97	-2.735
7	212.18	221.09	13.44	-2.967
8	28.08	216.48	12.43	-1.851
9	210.61	23.09	9.68	-0.914
10	161.86	45.97	7.74	-1.86
11	188.8	73.34	6.33	0.085
12	175.31	29.75	6.26	0.999
13	135.72	213.91	6.23	0.999

図 5 Keypoint information of chest_x-ray.bmp: position, scale and orientation

algorithm in Lowe's work to detect keypoints as the reference. To detect a feature of an image, the keypoint descriptor is created. A 16*16 neighborhood around the keypoint is taken and then divided into 16 sub-blocks of 4*4 size. A total of 128 bin values are available to represent as a vector to form keypoint descriptor, including keypoint position $(x_i, y_i), 0 \leq i \leq N$, scale, and orientation assignment. When the scale value is larger, the larger range of feature the image that the key-point represent. To give an example, we detected the SIFT keypoints in chest_x-ray.bmp from SIDBA image database, which is shown in Fig. 4. There are 409 keypoints detected, and the information is listed up as plotted in Fig. 5 with the following data accordingly: $x_i, y_i, 0 \leq \imath \leq 409$, scale and orientation assignment. There are 409 rows of positions information, a part of which are selected to hide confidential and sensitive personal information. The histogram of chest_x-ray.bmp is plotted in Figure. 2.1. According to this figure, we notice that most of the value located in the range of $[200, 250]$, which means it is convenient to embed information in each 8 bits as 256 is represented by 2^8. The histogram of scale is plotted in Fig. 6 (b). Most of values are concentrated among [0:3]. Being different from the mechanism of selecting positions for embedding information in conventional works, such as (1) using the point directly; (2) using the positions in a circle; or (3) applying DWT to positions. We apply an algorithm of reversible integer rotation to the selected x_i, y_i to get the positions for embedding payload.

2.2 Reversible positions rotation

Keypoints will be more robust against estimation after being applied transforming or rotation in a geometric. In work [19], a changing of spatial positions of camera optical axis to simulate different viewpoints of images to extract feature points from the stego data. In this work, angle α with matrix multiplication with $sin()$ and $cos()$. However, if the changing is not reversible, the original keypoints positions are not available. Thus, in this work, a reversible modified rotation algorithm applied to SIFT keypoints is proposed.

The algorithm is expressed in the following formula. Given $\begin{bmatrix} x_i \\ y_i \end{bmatrix}$ as one of the original keypoints and suppose $\begin{bmatrix} x_i' \\ y_i' \end{bmatrix}$ as the keypoints after rotation. The rotation computing is applied as follows:

$$\begin{bmatrix} x_i' \\ y_i' \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \quad (1)$$

In order to keep the reversibility of the original keypoints, the lifting and rounding computing are applied. For this process, there is a polynomial decomposition to represent the factor matrix as:

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} = round(R_1) \times round(R_2) \times round(R_3) \quad (2)$$

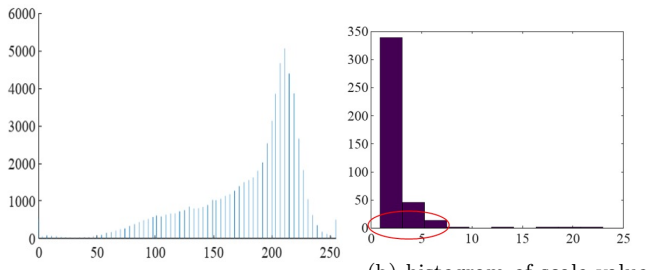
Here, $R_1 = \begin{bmatrix} 1 & \frac{-\cos\alpha - 1}{\sin\alpha} \\ 0 & 1 \end{bmatrix}, R_2 = \begin{bmatrix} 1 & 0 \\ -\sin\alpha & 1 \end{bmatrix}$, and $R_3 = R_1$.

2.3 Embedding Process

The flow chart of the proposed method, including embedding information and extraction with positions applied reversible rotations, is plotted in Fig. 7. There are two main steps for embedding.

Step 1: select hiding positions:

Detect the feature value of medical image with key points (x_i, y_i) using Lowe's algorithm [20][21]. The scale are in a descending order for these feature points. On purpose of compare the effectiveness of hiding positions, we specify five patterns of key-points for embedding for 16 bits. (a) first-coming 16 key-points with largest scale



(a) histogram of chest_x-ray.bmp (b) histogram of scale value

図 6 Histogram of original image and the scalue value

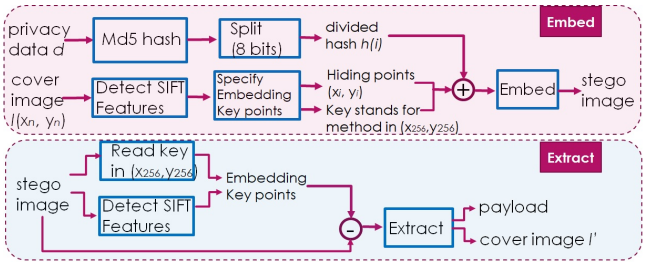


図 7 The flowchart of the proposed method

value: $(x_1, y_1), \ldots, (x_{16}, y_{16})$; (b) the last 16 key-points with lowest scale value: $(x_{409}, y_{409}), \ldots, (x_{394}, y_{394})$; (c) adjacent points to median value; (d) adjacent points to mode value (most frequent value); and (e) the proposed method: rotation with angle α: $\alpha = 5$, $\alpha = 10$, and $\alpha = 20$ adjacent to mode points, and $\alpha = 5$, $\alpha = 10$, and $\alpha = -10$ adjacent to median points. Since the key-positions are with feature value, the rotation may be a reasonable solution to avoid these point in a confidential way.

Step 2: embedding the payload

Hash value is generated by hash function applied to patients' personal data in DPC database, including ID (index), age, and operation code, generated by md5 algorithm, with a length of 256 bits. The hash string is going to be divided into 16 subsets, and then embedded in to the selected locations in the original image.

The extraction progress is a reverse process to the embedding process to extract data, and to reconstruct the payload in order. The hiding positions can be share between the trusted users, and patterns (a)-(d) can be calculated by the Lowe's algorithm. The proposed method for pattern (e) is confidential for the hiding positions, with the parameter α and the reversible rotation algorithm. The extraction algorithm, including these parameters should be shared in advance between the trusted sender and receiver.

The selected positions for embedding the payload by different patterns (a)-(e) are plotted in Fig. 8.

3. Experimental results

3.1 Evaluation benchmark

In order to evaluate the image quality, computing complexity, we use three benchmarks here for the evaluation: PSNR (Peak signal-to-noise ratio) [dB], computing time, and the entropy.

The environment for the implementation and experiments are listed in Table. 1.

Figure 9 plots the stego data generated by different patterns for hiding position selection. The difference between the original data and stego data when rotation ($\alpha = 5$) is applied to key-points which are adjacent to median value ($\alpha = 5$) is also plotted. According to the stego data, it is different to distinguish the difference comparing to the original data by human visual system. However, the noise is easier to be noticed when ($\alpha = 10$ (mode)).

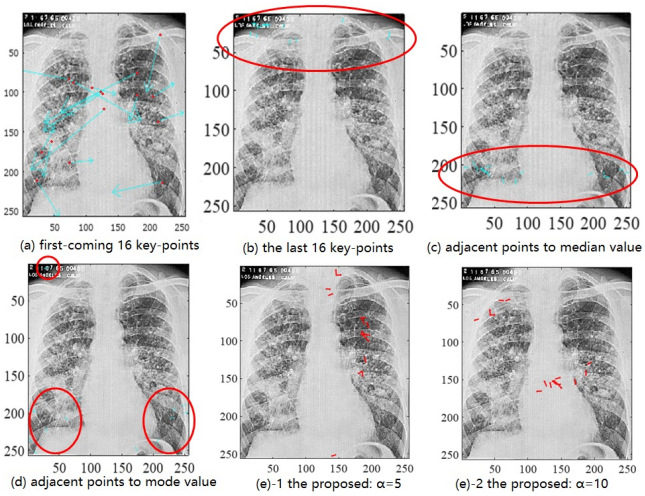


図 8 The selected positions for embedding the payload

表 1 Computing environment

Computer	Intel(R) Core (TM) i3-8100 CPU@ 3.6GHz
Programming	Matlab (Octave Ver. 5.1.0.0)

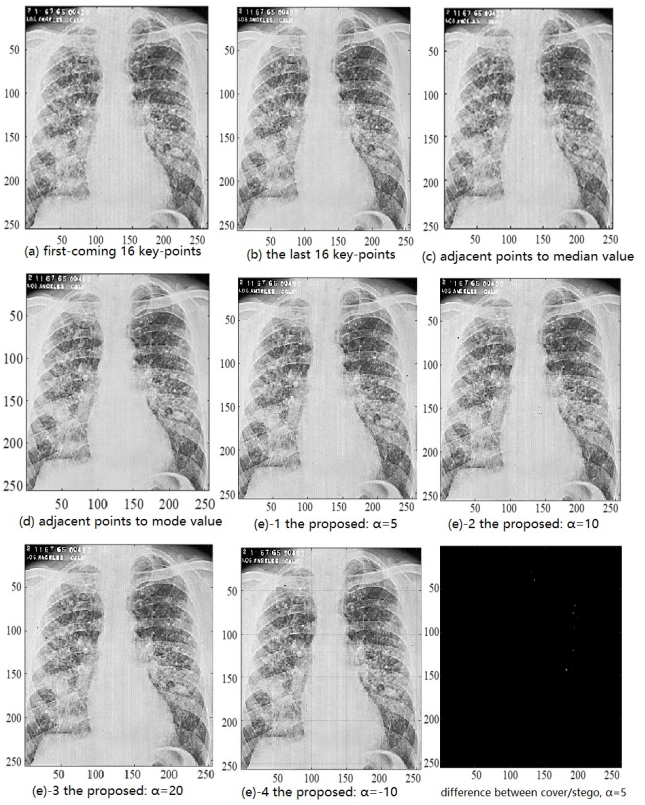


図 9 Stego data and the difference

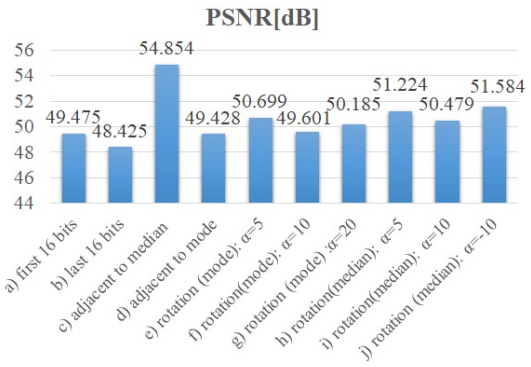


図 10 PSNR of the stego data

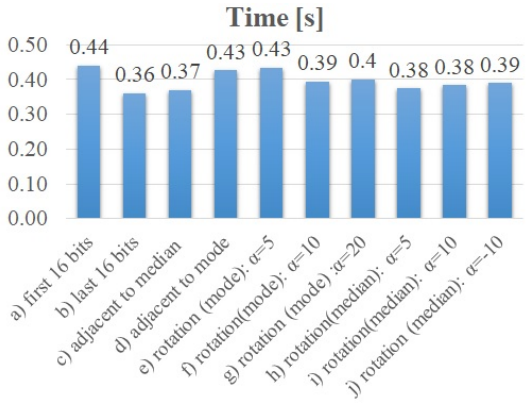


図 11 Computing time

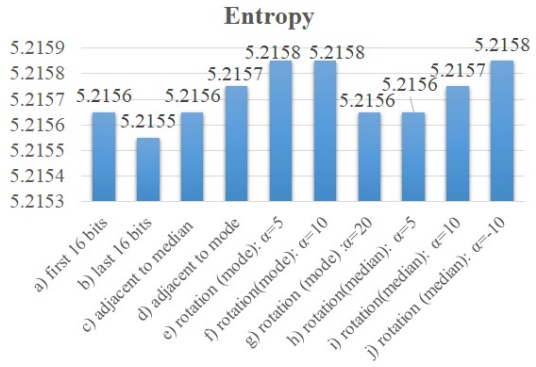


図 12 Comparison on entropy

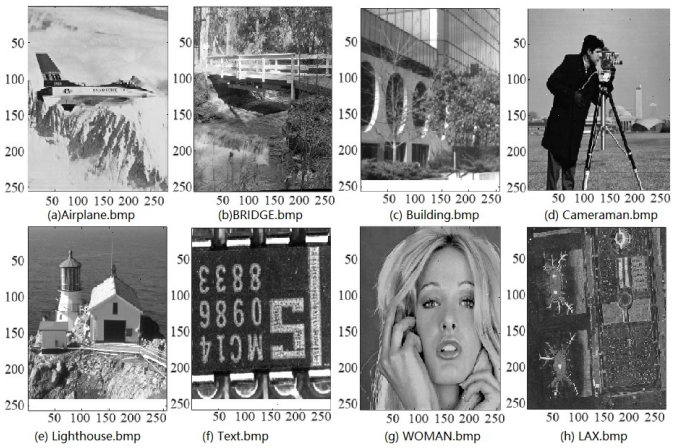


図 13 Stego data of SIDBA: rotation (median, $\alpha = 5$)

To evaluate the effectiveness, we also evaluate the stego data by rotation applied to key-points which are adjacent to mode value, as well as the median value.

The PSNR values are plotted in Fig. 10. Embedding to positions adjacent to median has the best quality that psnr = 54.854, with an average of 50.595 dB for different embedding positions. The proposed rotation method has better quality than the traditional first-coming, last and mode positions. After applying rotation, the best quality if rotation applied to mode positions with $\alpha = -10$. However, the worst PSNR after rotation is 49.601, which indicate an imperceptible degradation of the stego data after embedding. α should be explored in more angles, if the target application is for imperceptible purpose.

Figure 11 plots the calculation time for the processing. The process completed in an average of 0.397 s. Fig. 12 plots the entropy of the stego data. The entropy is calculated by: $entropy = -\Sigma(P. * \log_2 P)$, where P is the distribution of the elements of image. The smaller the value is, the result is better. According to Fig. 12, for rotation algorithm, the rotation applied to adjacent positions to median key-points while $\alpha = 5$, and adjacent points to mode key-points while $\alpha = 20$ have the best effectiveness, where $entropy = 5.2156$.

However, this method may dependent to the coefficient of original images. As a reference, the stego of SIDBA (Standard Image Data-BAse) applying rotation to adjacent positions to median key-points ($\alpha = 5$) is plotted in Fig. 13.

4. Conclusion

This paper proposed an novel digital watermarking algorithm to specify the embedding positions by applying a reversible rotation to SIFT feature key-points. Experimental evaluation results on image quality, computing time, and the entropy show the proposed method is a imperceptible method, with an average of 50.595 dB in PSNR; a fast algorithm, with an average of 0.397 s for computing; and a lossless method with an average of 5.216 in entropy. The best positions and angle for rotation is the key-points adjacent to the mode, with the angle $\alpha = -10$ for PSNR. We list up a more sophisticated algorithm for embedding as the future work for stronger robustness, such as coefficients expansion after applying an integer and reversible discrete cosine transform to the value in the image, or exploring hiding payload into residue data after applying linear prediction coding, etc. Effectiveness

evaluation to the real dataset, comparing to the conventional data, and the application to solve the social problem is another task in the short future.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP18K18052.

参考文献

[1] Simon, E., Paoletti, N., et, al.: Broken Hearted: How To Attack ECG Biometrics. In: Proc. of NDSS 2017, pp. 1-15, USA (2017).

[2] Kikuchi, H., Huang, X., et, al.: Privacy-Preserving Hypothesis Testing for Reduced Cancer Risk on Daily Physical Activity. In: Journal of Medical Systems (Springer Nature), vol. 42, Issue. 90, pp. 1-12, (2018)

[3] Huang, X., Kikuchi, H., Fan C.: Privacy preserved spectral analysis using IoT mHealth biomedical data for stress estimation. In: Proc. of the 32nd IEEE International Conference on Advanced Information Networking and Applications (AINA), pp: 793-800, Poland, (2018)

[4] Kikuchi H., Yasunaga H., et, al.: Efficient Privacy-Preserving Logistic Regression with Iteratively Reweighted Least Squares. In: Proc. 11th Asia Joint Conference on Information Security, pp. 48-54 (2016)

[5] Kikuchi, H., et, al.: Privacy-Preserving Multiple Linear Regression of Vertically Partitioned Real Medical Datasets, In: Proc. of AINA, pp. 1042-1049 (2017)

[6] Ito, S., Harada R,. et, al.: Risk of Reidenti cation from Payment Card Histories in Multiple Domains, Proc. of AINA (2018)

[7] Dwork, C., Roth, A.: The Algorithmic Foundations of Differential Privacy. In: Foundations and Trends in Theoretical Computer Science: Vol. 9: No. 34, pp 211-407 (2014)

[8] Dwork, C.: Differential privacy. In: Proc. of ICALP, pp.1-12 (2006)

[9] Wang, Y., Si, C., Wu, X.: Regression Model Fitting under Differential Privacy and Model Inversion Attack. In: Proc. of IJCAI, pp. 1003-P1009 (2015)

[10] Huang X.: Mechanism and Implementation of Watermarked Sample Scanning Method for Speech Data Tampering Detection. In: Proc. of ACM 2nd International Workshop on Multimedia Privacy and Security (MPS) in CCS, pp. 54-60, Canada (2018)

[11] Huang, X., Ono, N., et, al.: Reversible Audio Information Hiding for Tampering Detection and Localization Using Sample Scanning Method. In: Journal of Information Processing, vol. 25, Issue. 2017, pp. 469-476 (2017)

[12] Yang, B., Schmucker, M., Niu, X.M., Busch, C. Sun, S.G.: Reversible image watermarking by histogram modification for Integer DCT coefficients. In: Proc. Workshop on Multimedia signal processing, pp.143-146 (2004)

[13] Lin, C.C., Shiu, P.F.: High capacity data hiding scheme for DCT-based images. In: Journal of Information Hiding and Multimedia Signal Processing, vol.1(3), pp.220-240 (2010)

[14] Yan, D.Q., Wang, R.D.: Reversible data hiding for audio based on prediction error expansion. In: Proc. International Conference of Intelligent Information Hiding and Multimedia Signal Processing, pp. 249-252 (2008)

[15] Hayashi, M., Kawamura.M.: Improved SIFT Feature-Based Watermarking Method for IHC Ver. 5. In: Proc of APSIPA ASC, pp. 1536-1543 (2018)

[16] Uchida, K., et, al.: Evaluation of SIFT feature based watermarking method for scaling attack. In: Proc. Technique report of IPSJ, vol. 114, no. 511, EMM2014-83, pp. 37-42 (2015)

[17] Liu, J., Li, J. et, al.: Medical Image Watermarking Based on SIFT-DCT Perceptual Hashing. In: Proc of International Conference on Cloud Computing and Security, pp. 334-345, 2018

[18] Singh K.: A robust rotation resilient video watermarking scheme based on the SIFT. In: Proc. of Multimedia Tools and Applications, vol. 77 (13), pp. 16419–16444 (2018)

[19] C.Y. Wang, et, al.: Robust Image Watermarking Algorithm Based on ASIFT against Geometric Attacks. In: Applied Sciences, pp. 11-19 (2018)

[20] D. Lowe.: Distinctive image features from scale-invariant keypoints. International Journal of Computer Vision, vol. 60(2), pp. 91-110 (2004)

[21] D. Lowe.: Object recognition from local scale-invariant features. International Conference on Computer Vision, pp. 1150-1157 (1999)