Vol.2020-CSEC-90 No.15
Vol.2020-SPT-38 No.15
2020/7/20

スペクトル領域上の雑音摂動法における雑音抑圧手法

黄　緒平[1,a)]　川島　龍太[2,b)]

概要：近年，ウェアラブル IoT 機器に多様なセンサーが内蔵され，安価でかつ高精度に生体計測できるようになった．一方，脈拍等センシティブな生体情報の悪用が社会問題となっている．特に，生体情報から持病の推定や心拍数情報を用いたユビキタス IoT デバイスの生体認証システムへの攻撃等が挙げられる．時系列データへの差分プライバシーにおける雑音摂動が有効であるが，複数のプロバイダーによるデータ収集において雑音が大きくなり，誤差を引き起こす問題がある．本研究は，生体情報の時系列データを対象に，整数離散コサイン変換を用いたスペクトル領域上の雑音摂動メカニズムによって雑音を生成する手法を提案する．評価手法として，スペクトル領域 Gaussian ノイズ及び Laplace ノイズを時間領域にて生成し，雑音摂動後の脈拍データを用いてストレス推定を行い，生データによる計算結果と比較する．

キーワード：雑音摂動, 雑音抑制, スペクトル領域, IoT 生体情報

1. Introduction

1.1 Background

Numerous companies collect personal information for medical treatment or data analysis in hospitals or research institutes, including personal sensitive information and bio-information. Even though in most of situations, these data are maintained, restored, and shared among instituted, with benefit as a significant medical reference, are valuable and publicly available for research purpose. Nevertheless, since most of these data are sensitive personal data, malicious users may abuse these data without the permission of the patients, or sell these consumer information to the third party. Thus, policies or technology solutions are required to preserve the privacy of individuals who contributed these data from being specified by hack or statistical methods.

Meanwhile, with the highly developed IoT devices and data transmitting technology, personal bio-information is available ubiquitously and conveniently, and shared by wearable IoT devices easily, e.g. smart watch, IoT band, portable devices with sensors for bio-information for the purposes of fit, health care, daily management, etc. Some of these devices collect bio-information precisely with variable bio-sensors. Thus, these IoT devices has been an alternative solution to provide an indications of health as a reference. These data include GPS, heart rate, sleep stages, δ oxy-Hb (a.u) underneath the skin, breath, blood pressure, etc. Because the convenience to get data automatically within a certain time interval, and it is free burden for measure, this devices are widely used.

However, with the development of IoT authentication, the dynamic heart rate collected by Nymi band can be used for authentication to unlock ubiquitous IoT devices [1]. the authentication is convenient, since the bio-information the specific individuals can be used as the key or password. However, there is a risk of abuse and endanger the authentication system that in work [1], a simulation for attack successes by representing heat beat from ECG monitor for impersonation, which means the system is not reliable, and solutions are required to protect the data from abuse.

There are also other conditions indicate the risk to disclose the daily personal information to the third party. For example, daily lifelog is available by analyzing the electric power [2], and chronic disease can be estimated by heart rate variability (HRV) [1], which should be protected since remote on-line clinic has becoming popular.

From the reasons of above, it is risky to supply of raw

[1] 東京都立産業技術大学院大学
東京都品川区東大井 1-10-40, 1400011
[2] 名古屋工業大学
愛知県名古屋市昭和区御器所町, 466-8555
[a)] huang-xuping@aiit.ac.jp
[b)] kawa1983@nitech.ac.jp

data, and there are requirements to preserve the confidentiality and the privacy utility of bio-information, as well as ensuring the usability of the original data.

1.2 Conventional works and motivation

There are three main solutions to preserve the privacy of sensitive data:

I. Secure computation 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. The advantage is that the security is guaranteed and it is useful for calculation and analysis with data in distributed institutes. However, the disadvantages are (1) data sharing protocol is required for secure multi-parties computation; and (2) high computing performance is necessary, since homomorphic encryption may enlarge a 1 bit data into 1MB.

II. Data anonymization This solution mainly focus on removing personally identifiable information by suppression or generalization using *k-anonymity, l-diversity, t-closeness* [6]. There is a trade-off between confidential and data usability, since the irreversible data loss for anonymization process. Another point is that it depends on the background knowledge of an adversay that the attackers have for assumptions and inferences to specify a individual.

III. Differential privacy This alternative solution guarantee the confidentiality by adding noise with sensibility, which is corresponding to queries or operations [7], [8], [10], [11], [12], **?**. Noise is generated by a particular mechanism considering both of security utility and usability. Security is guaranteed by utility ε.

In work [2], Gaussian noise was added to the electric power. We mainly focus on noise perturbation considering the concept of local differential privacy in this paper. In case of protecting the security of distributed data, by perturbing noises to every time series data collected from multiple providers, deterioration of the accumulated data becomes large, which may influence the analysis results. Thus, algorithm to generate a noise with low distortion with high usability, and high utility are necessary.

Differential privacy solutions in the frequency have been proposed [11], [12], using FFT and Haar wavelet transform, however the distortion, and the uncomputable to sparse and negative data are still challenging.

1.3 Our contribution

In this work, we propose a noise generation mechanism based on spectral differential privacy using integer DCT to transform data from the time domain into the frequency domain, and perturb the noise into bio-metric domain, including voice and heart rate, in order to ensure both of the privacy utility and usability. Laplace noise in terms of the proposed mechanism are generated and perturbed in the frequency domain. Distortion has been evaluated and a comparison between Gaussian noise is also given to verify the effectiveness of the distortion suppression.

This paper is organized as follows. The approaches taken here and those of previous studies are discussed in Section 1. Sections 2 discusses spectral analysis for stress estimation and health care using IoT data. Section 3 describes the proposed method and implementation in detail. Section 4 describes experimental evaluation results. We conclude the paper in Section 5.

2. Spectral analysis for stress estimation

2.1 Dataset

Heart rate $x(t)$ ($x, t \in R$, [bpm]) in time sequence is collected by Fitbit Charge 2 during 7/3-7/12, 7/28-7/30, 2018 with 5 participants ages around 20's (female and male), 30's (female) and 50's (male). Time t is with an interval of 1 minute. RRI (RR Interval) is calculated by $\frac{60}{x(t)} * 1000$ (ms).

2.2 Heart rate variables for healthcare

HRV is a reference for healthcare, including improving the sleep quality, and for advices for daily fitness and ability. Figure 1 plots an example of HRV corresponding to daily activities. The data was collected by Fitbit Charge 2 on 29, June 2018, by the 50's male participant. Heart beat gets faster during drinking, and then decrease to be stable after 10 mins. Two peak HRV around the 100 and 150 mins after drinking may involved to walking home and daily activities before sleep.

Besides analysis in the time-series, spectral analysis is also focused on as an stress estimation index.

2.3 Stress index

Power spectral density (PSD, $[ms^2/Hz]$) analysis of heart rate has been used as the stress index to calculate the ratio between low frequency (LF) and high frequency (HF) components as: $P(\omega)_{LF} = \int_{0.04}^{0.15} S(\omega) * \frac{\Delta\omega}{2} d\omega$, $P(\omega)_{HF} = \int_{0.15}^{0.4} S(\omega) * \frac{\Delta\omega}{2} d\omega$,where $\omega = \frac{2\pi}{T}$ and $\Delta\omega =$

$\frac{1}{length(\omega)}$. Stress index is estimated by $ratio = \frac{P(\omega)_{LF}}{P(\omega)_{HF}}$ Here, power spectral $S(\omega)$ can be obtained by processing FFT to autocorrelation function $C(\tau)$ as: $S(\omega) = \lim_{T\to\infty} \frac{2\pi|X(\omega)|^2}{T}$. In case that most of PSD values concentrated in higher frequency domain and peak value is detected in higher value, it indicated parasympathetic dominance (relaxing). Oppositely, if the peak value of PSD located among LF domain, it indicated sympathetic dominance (stressful). The lower the *ratio* is, the more relaxing it indicated. Stress is estimated from result of *ratio* as defined in work [14] that (1) *ratio* ∈[0, 0.8]: *relaxing*, (2) *ratio* ∈[0.8, 2]: *normal*; and (3) *ratio* >2: *stressful*. Figure 13 plots an example of spectral analysis result for stress estimation in different window lengths, using the data of 30's participant (female) on 30, July 2018. The results indicate a relaxing statues of the participant by low LF/HF value.

3. Mechanism of noise perturbation in spectral domain

3.1 Details of integer DCT IV (intDCT)

Let

$$x = \{(x_1), (x_2), \dots (x_n)\}^T \quad (1)$$

$$X = \{(X_1), (X_2), \dots (X_n)\}^T \quad (2)$$

be a time-domain signal at an N-point frame and its DCT coefficients, respectively. In a continuous case, we can obtain DCT coefficients X from a time-domain signal x by DCT matrix as

$$X = C_N^{DCT-IV} x \quad (3)$$

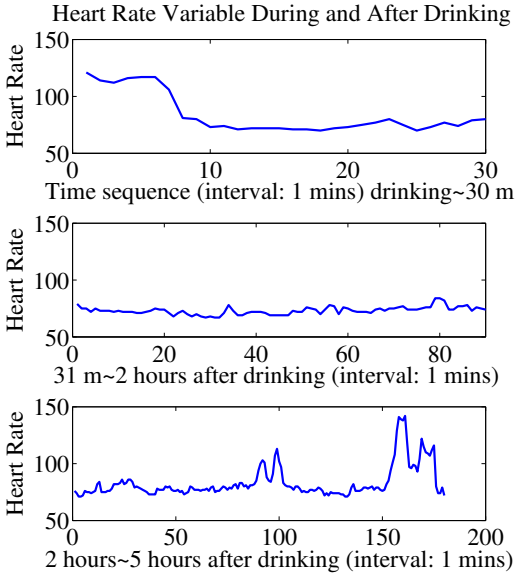

図 1 An example of heart rate variability (HRV) corresponding to daily activity (drinking)

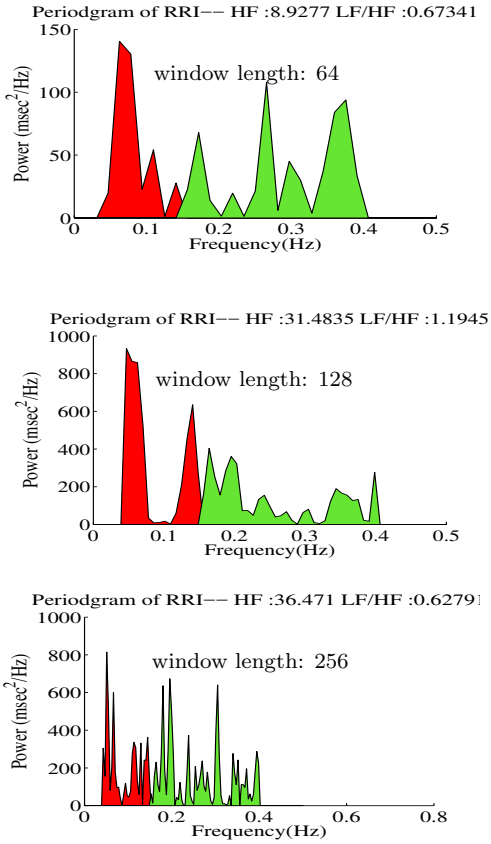

図 2 Periodgram in different window lengths

where the (i,t)-th $(1 \le i \le N,\ 1 \le t \le N)$ elements of the DCT matrix. C^{DCT-IV} are represented as

$$C_N^{DCT-IV}(i,t) = \sqrt{\frac{2}{N}} \left[\cos\left(\frac{(t+\frac{1}{2})(i+\frac{1}{2})\pi}{N}\right)\right]. \quad (4)$$

For lossless audio coding, intDCT has been proposed in [13]. In this process, the integer signal in the time domain is transformed into integer DCT coefficients in a reversible way. This DCT matrix can be factorized into the product of block triangular matrices with block identity diagonals. Multiplying a triangular matrix followed by a rounding operation can be reversible even if elements of the triangular matrix are not integers. This also holds true in the block matrix case. Therefore, iteratively multiplying triangular matrices in order and applying the rounding operation can be completely reversible. Even though Expectation Maximization (EM) algorithm can be used to de-noise, reversibility makes it convenient and possibility for further re-identification.

There is a feature of intDCT IV for the data transform that when the frequency domain increases, the value of DCT coefficients decreases generally. Figures 3,4,5,6, show an example of RRI plotted in the time domain and in the frequency domain as DCT coefficients. Figure 3 plots an example of heart rate variability in RRI

[ms] on 30th, July 2018, including 1536 samples, with a $\overline{RRI} \pm \sigma = 784 \pm 3.65$. Figure 4 is the DCT coefficients corresponding to the RRI value. In the low frequency domain, the DCT coefficients have values indicating higher amplitude. Figure 5 plots a subset of DCT coefficients in the low frequency domain with DCT index ranges [1:200], where the maximum DCT coefficients as 28556, and the minimum absolute value is 0. Meanwhile, most of the DCT coefficients have small values in the DCT coefficients index [200:1536], which covers values as 31 ± 26, where the mode value is 19, and the middle value is 24. The DCT coefficients have more smaller values than that in the time domain. Since the noise is perturbed to the original data, thus the distortion of noise may be suppressed by noise perturbation in the frequency domain rather than in the time domain theoretically.

However, the logic for noise generation is important, and it is depended on the signal processing of data transform algorithm from the time domain to the frequency domain. Work [13] indicates the algorithm requires the process of intDCT-IV as $2.5n \log_2^n - n$ for each n-sized frame.

3.2 Noise assignment in Laplace distribution for *L*1-sensibility

Given the original heart rate data in time series are $D = \{x_1, x_2, \ldots, x_n\}$, and the attacker has the data series as $D'' = \{x_1'', x_2'', \ldots, x_n''\}$, if and only if dataset D and D'' differ in one element. This is called L1-sensitivity.

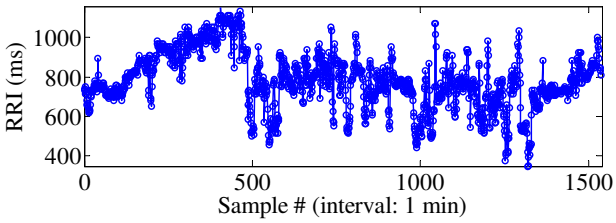

図 3 Time-series RRI (ms): 1536 samples on 30, July

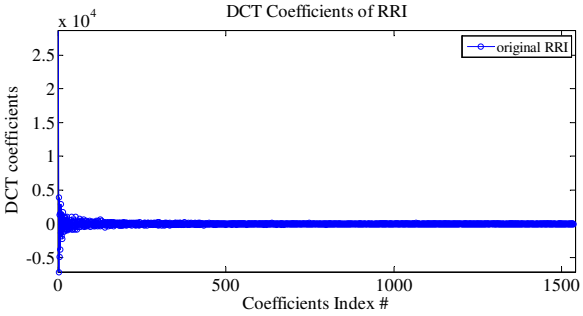

図 4 DCT coefficients of RRI: 1536 samples on 30, July

The L1-sensitivity $\Delta_{1,q} = max_{D \sim D''} ||q(D) - q(D'')||_1$ indicates the situation that when error between $q(D)$ and $q(D'')$ is maximal. Then the mechanism for perturbation

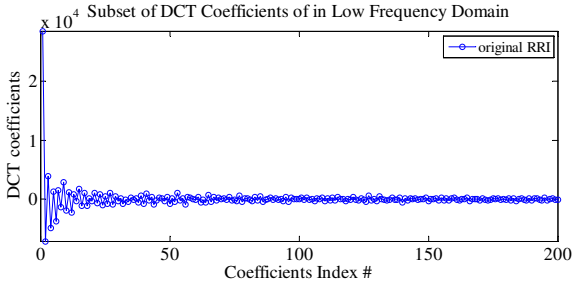

図 5 subset of [0,200]-th coefficients in the low frequency domain

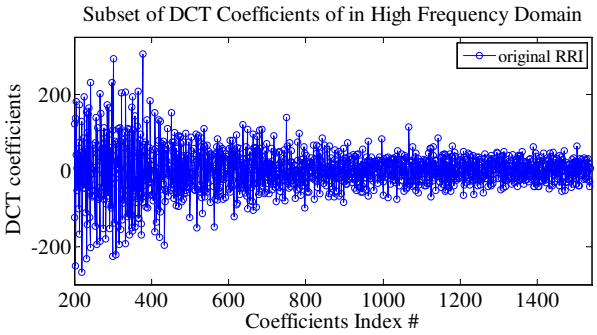

図 6 subset of [200,1536]-th coefficients in the high frequency domain

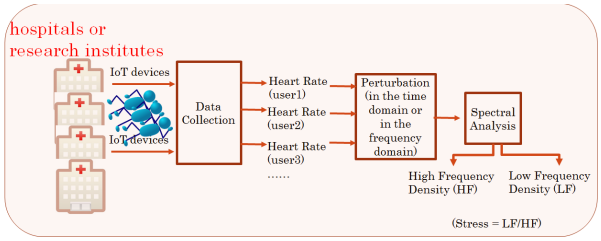

図 7 Flow chat of noise perturbation in the frequency domain for stress estimation for distributed data

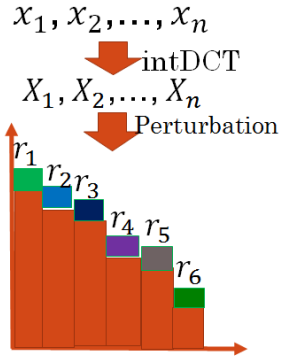

図 8 Illustration for noise perturbation to DCT coefficients

$\lambda = \Delta_{1,q}/\varepsilon$. Here, the smaller the privacy utility ε is, the stronger the privacy is guaranteed. Meanwhile, the distortion should be controlled to be as small as possible to achieve the higher usability of the data.

According to the calculation requirement of intDCT, $2.5n\log_2^n - n$ is necessary for the process. Suppose the probability of each sample out of n-point to be disclosed is $\frac{1}{n}$, then the noise mechanism corresponds to $(2.5n\log_2^n - n) \times \frac{1}{n}$, then $\lambda = (\log_2^n)/\epsilon$.

3.3 Algorithm of noise perturbation based on intDCT

In the scenario to collect data and apply noise perturbation to the time-series domain towards distributed data, the accumulated noise is getting larger. Figure 7 illustrates this use case. In order to suppress the degradation of noise perturbed, a noise mechanism based on intDCT calculation and correspond to Laplace distribution is generated according to the algorithm as follows:

The algorithm to calculate stress index with noise perturbation in the frequency domain based on intDCT is listed as follows:

Input: $D_i = \{x_1, x_2, \ldots, x_n\}, (1 \le i \le n)$

Output: $D_i' = \{x_1', x_2', \ldots, x_n'\}$ in the time domain.

step 1 Transform D_i to generate $dct(D_i)$ to get $X_1, X_2, \ldots, X_n$ in the frequency domain using intDCT.

step 2 Specify privacy utility ϵ (e.g. $\epsilon = 0.1, 0.15, 0.2\ldots$) to generate Laplace noise mechanism $\lambda = \Delta_{1,q}/\varepsilon$ to generate the noise according to Laplace distribution as $r_i = \frac{1}{2\lambda}e^{\frac{-|x|}{\lambda}}$, here $\Delta_{1,q}$ is the mechanism which is related to integer DCT transform that $\Delta_{1,q} = \log_2^n$, here n is the length of data; and then specify δ=0.05.

step 3 Perturbation: $\widetilde{D_i} = X_i + r_i$

step 4 Perform invise DCT $idct(\widetilde{D_i})$ to get $\{x_1', x_2', \ldots, x_n'\}$.

Then spectral analysis is applied to $\{x_i'$ to calculate the stress index in a $(\epsilon, \delta)-$differential privacy preserved way. Please refer to our previous work [15] for the details of proof of (ε)-differential privacy for assigned noise in the frequency domain.

Figure 8 illustrates the algorithm of noise perturbation to DCT coefficients.

4. Experimental Results

4.1 Evaluation criteria

In these paper, two criteria are used to evaluate the precise and effectiveness of noise perturbation: (1) stress index results are calculated comparing to the values calculated using raw data, and (2) Mean Squared Error (MSE). In the conventional works, MSE is also used as a evaluation criteria [12] that when MSE decreases, the usability increases. In this paper, MSE is calculated by:

$$\frac{1}{n}\Sigma_{i=1}^{n}(\widetilde{D_i} - D_i)^2 \quad (5)$$

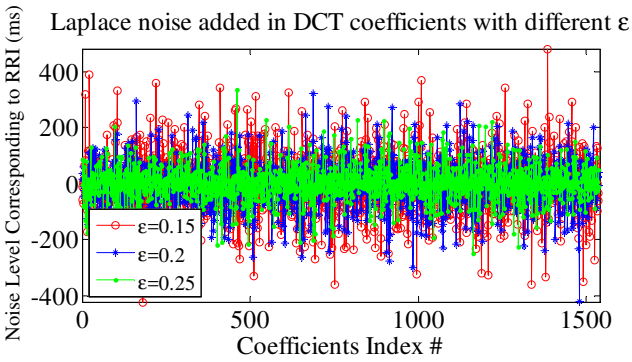

図 9 Laplace noise with different ε corresponding to DCT coefficients in the frequency domain

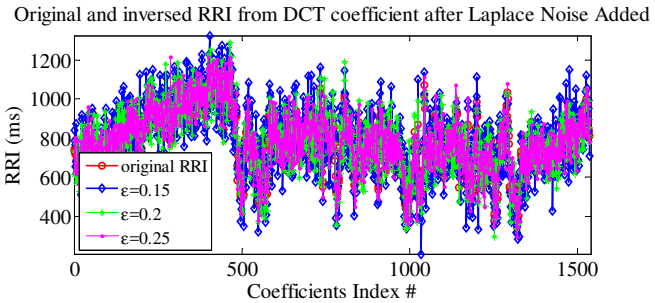

図 10 Inversed RRI from DCT coefficients after Laplace noise perturbed in the frequency domain

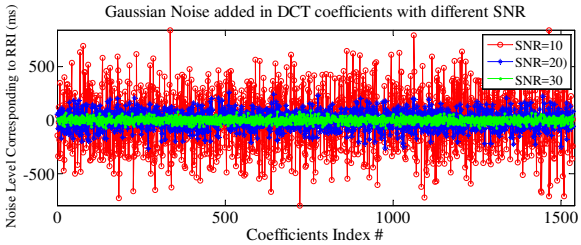

図 11 Gaussian noise corresponding to DCT coefficients with different SNR in the frequency domain

4.2 Perturbation by Laplace noise with different privacy utility ε

Noise generated by the mechanism $\lambda = (\log_2^n)/\varepsilon$, according to Laplace distribution is $r_i = \frac{1}{2\lambda}e^{\frac{-|x|}{\lambda}}$. Figure 9 plots the Laplace noise with different ϵ. It is obvious that when the privacy utility is stronger (ε is smaller),

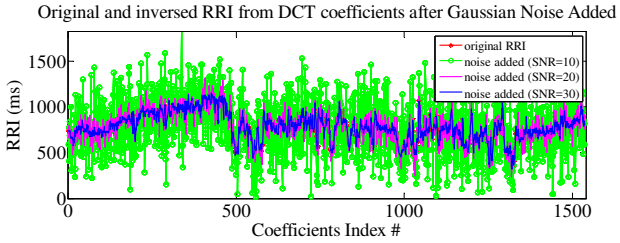

図 12 Inversed RRI from DCT coefficients after Gaussian noise perturbed in the frequency domain

the noise is larger and may affect the statistics analyzing result for knowledge mining, which is a tradeoff by noise perturbation. Figure 10 plots the inversed RRI in the time domain, transformed from the frequency domain after Laplace noise perturbation with spectral differential privacy. Accordingly, smaller ε has larger noise values perturbed.

4.3 Perturbation by Gaussian noise with different Signal-to-Noise (SNR)

Comparing to Laplace noise generated by the proposed spectral differential privacy mechanism, Gaussian noise perturbed to the signal in the spectral domain is also implemented. Figure 11 plot the Gaussian noise added in DCT coefficients with different SNR values. It is obvious that higher SNR ensures lower distortion and smaller noise. By comparing the value in y-axis to that in Figure 9, the noise generated by Laplace distribution is smaller than that generated by Gaussian noise in the frequency domain. Figure 12 plots the inversed RRI in the time domain, transformed from the frequency domain after Gaussian noise perturbation. Accordingly, the values of RRI with noise perturbed in Figure 10 (Laplace noise with spectral DP) are smaller than that in Figure 12 (Gaussian noise with spectral DP).

4.4 MSE and stress index results of noise values

In order to compare the effectiveness of noise suppression by spectral differential privacy mechanism (Laplace), MSE and stress index for analyzing heart rate data on Jun 18, 2018 are used for the comparison. The result is listed in Table 1.

According to the result in Table 1, MSE after Laplace noise perturbation generated by spectral differential privacy has smaller noise than that of Gaussian noise, which means the proposed method is effective for noise suppression. Stress index results show that the proposed method has closer results to original data, even with the highest

表 1 MSE and MSE and stress index results by Laplace and Gaussian noise generated by spectral differential privacy

Data	noise level	Stress index	MSE
original data	null	0.405	null
Gaussian noise perturbed	SNR=10dB	0.168	8.6125e+04
	SNR=20dB	0.423	2.9694e+04
	SNR=30dB	0.405	1.7320e+04
Laplace noise perturbed	ε=0.5	0.443	7.5340e-04
	ε=0.75	0.443	4.3965e-04
	ε=1	0.443	2.4687e-04
	ε=1.25	0.443	1.3341e-04

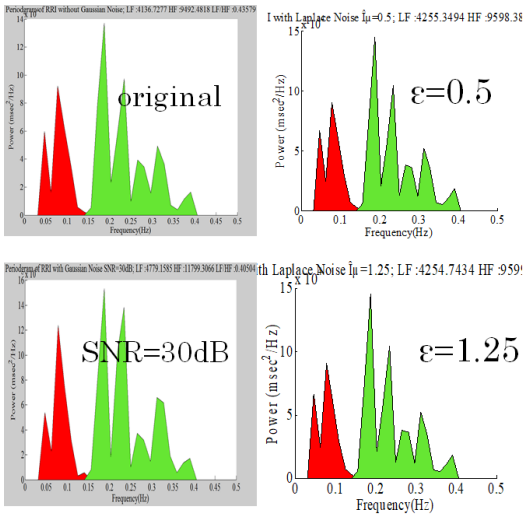

図 13 Stress index result after noise perturbation by the proposed method

security utility level when ε=0.5.

Figure 13 plots the stress index result after noise perturbation by the proposed method and the Gaussian noise. The stress estimation has a similar results after noise perturbation generated by the proposed mechanism based on spectral privacy preserving.

5. Conclusion

This paper proposed a new noise suppression method based on spectral differential privacy for data privacy preserving. This method can be applied to data analysis on spectral domain, such as stress estimation, and disease prediction by autoregressive in the frequency domain. This supplies an alternative data analyzing methods besides the linear and logistic regression. The Laplace noise generated according to the mechanism of spectral differential privacy promises a smaller noise than the Gaussian noise, while the security utility ε is guaranteed, as well as the stress estimation results be similar to the original data without noise perturbation approximately. The fu-

ture work is to apply this method to a big amount of data to check the effectiveness and to improve the noise generation mechanism for more data analysis models. Exploring to various regression algorithms to solve different social problems is listed as another future task.

謝辞 This work was supported by JSPS KAKENHI Grant Number JP18K18052. The research was supported by NII CRIS Contract Research 2019.

参考文献

[1] Simon Eberz, Nicola Paoletti, Marc Roeschlin, Andrea Patane, Marta Kwiatkowska, Ivan Martinovic, "Broken Hearted:How To Attack ECG Biometrics", Proc. of NDSS, pp.1-15, 2017

[2] M. Hattori. et al, "Yet Another Experiment on Privacy-Utility Tradeoff for Power Usage Data", Proc. of CSS2017, pp. 1350-1357, 2017

[3] H. Kikuchi, H. Yasunaga, H. Matsui, C, I. Fan, "Efficient Privacy-Preserving Logistic Regression with Iteratively Re-weighted Least Squares", Proc. 11th Asia Joint Conference on Information Security, pp. 48-54, (2016)

[4] H. Kikuchi, C. Hamanaga, H. Yasunaga, H. Matsui, and H. Hashimoto, "Privacy-Preserving Multiple Linear Regression of Vertically Partitioned Real Medical Datasets", Proc. of AINA 2017, pp. 1042-1049, 2017

[5] X. Huang, H. Kikuchi, and C. Fan, "Privacy preserved spectral analysis using IoT mHealth biomedical data for stress estimation", Proc. of AINA, pp. 793-800, 2018

[6] S. Ito, R. Harada, and H. Kikuchi, "Risk of Re-identification from Payment Card Histories in Multiple Domains", Proc. of AINA, 2018

[7] C. Dwork, and A. Roth, "The Algorithmic Foundations of Differential Privacy", Foundations and TrendsR in Theoretical Computer Science: Vol. 9: No. 3-4, pp 211-407, 2014

[8] C. Dwork, "Differential privacy", Proc. of ICALP, pp.1-12, 2006

[9] G. Zhou, et. al, "A differential privacy noise dynamic allocation algorithm for big multimedia data", Multimedia Tools and Applications Vol. 78, pp.37473765, 2019

[10] Y. Wang, C. Si, and X. Wu, "Regression Model Fitting under Differential Privacy and Model Inversion Attack", Proc. of IJCAI, pp. 1003-P1009, 2015

[11] V.Rastogi, and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption", Proc. of SIGMOD, pp.1-25, 2010

[12] X. Xiao, G. Wang, and J. Gehrke, "Differential privacy via wavelet transforms", Journal IEEE transactions on knowledge and data engineering, vol. 23(8), pp.1200-1214, 2011

[13] Haibin, H., Susanto, R., and Rongshan, Y, "A fast algorithm of integer MDCT for lossless audio coding", *Proc. IEEE International Conference on Acoustics, Audio and Signal Processing (ICASSP)*, pp.177-180 (2004)

[14] http://www.fatigue.co.jp/qa.htm, final access on 20th Jan, 2020

[15] X. Huang, "Watermarking based data spoofing detection against speech synthesis and impersonation with spectral noise perturbation", *Proc. IEEE International Conference on Big Data*, pp. 4600-4604, Dec 2018