The University of Osaka
Institutional Knowledge Archive

Title	Noise-Masking Cryptosystem Using Watermark and Chain Generation for EEG Measurement with Compressed Sensing
Author(s)	Yamamoto, Tomoya; Kanemoto, Daisuke; Hirose, Tetsuya
Citation	
Version Type	AM
URL	https://hdl.handle.net/11094/101386
rights	© 2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

Noise-Masking Cryptosystem Using Watermark and Chain Generation for EEG Measurement with Compressed Sensing

Tomoya Yamamoto, Daisuke Kanemoto*, and Tetsuya Hirose
Graduate School of Engineering, Osaka University, Suita, Japan
dkanemoto@eei.eng.osaka-u.ac.jp

***Abstract*—Achieving both low-power consumption and robust security is essential in wearable measurement devices such as electroencephalogram (EEG) headsets, which are highly anticipated in the consumer electronics field. To address these dual requirements, we focused on a compressed sensing-based security technique for chain-generated noise-masking, as proposed in prior research. In this paper, we explain the power consumption in relation to the circuit input range and resolution, with a focus on practical implementation. Based on simulations that assume continuous EEG data over a period of more than one week, we verify that when the compression ratio is four, the system is reliable and resistant to attacks when the watermark magnitude is set to $100\ \mu\mathrm{Vrms}$ and the pseudo-noise magnitude is at least $250\ \mu\mathrm{Vrms}$. Furthermore, simulations confirm no additional requirements for resolution or input range, which are closely related to the power consumption of the device, are necessary despite the insertion of watermarks and noise. Our research aims to advancement the field of smart healthcare through innovative contributions from the perspectives of low-power consumption and security.**

***Index Terms*—BSBL, compressed sensing, cryptosystem, EEG, low-power dissipation, secure communication, watermark**

I. Introduction

An electroencephalogram (EEG) is a crucial biosignal, and obtaining EEG information helps early disease detection [1] and has applications in brain–computer interface technologies [2]. Most existing EEG recording devices are wired. However, a non-invasive, long-operating wireless measurement system is required to expand the use of EEG in recording devices. Therefore, increasing research is being conducted on wearable wireless EEG devices for consumers that can utilize EEG signals in everyday life [3]. To realize such a system, it is necessary not only to acquire accurate data but also to accomplish low-power consumption and robust security. In this study, we focused on the compressed sensing (CS) technology [4] [5] using random under-sampling [6]. This technology is expected to achieve accurate data acquisition with low-power consumption because it enables high-precision reconstruction while reducing the amount of information handled by the circuits. Several studies have applied CS to the acquisition of biological signals [7], including ECG [8], EEG [9]. Furthermore, research on achieving low-power sampling using CS technology has advanced significantly. For example, by employing random under-sampling to enable low-power wireless EEG systems, studies demonstrated power-saving effects in analog-to-digital (A/D) converters [6], amplifiers [10] [11], and overall systems [12]. Additionally, previous studies have proposed the chained-generated noise-masking system [13], which leverages CS as a lightweight encryption method to enhance security. This study focused on a chained-generated noise-masking system. The chained-generated noise-masking system ensures security with minimal power consumption by inserting random pseudo-noise and digital watermarks as masks during the compression of acquired signals. However, if the insertion of masks requires a higher resolution and input range, it may challenge the balance between security and low-power consumption. This paper presents a more detailed design methodology for a chained-generated noise-masking system compared to previous research, and we evaluate and discuss its power consumption, recovery accuracy, and security strength.

The remainder of this paper is organized as follows: In Chapter II, we explain the foundational knowledge of CS and the chained-generated noise-masking system. Chapter III presents the design parameters of the proposed system. Chapter IV describes the simulation conditions, results, and corresponding discussion. Finally, Chapter V concludes the study.

II. Compressed Sensing and chain-generated noise-masking

CS is a technology that enables the accurate reconstruction of the original signal even when sampled at a frequency lower than the Nyquist frequency under the assumption that the signal is sparse.

A. Sparsity

Sparsity refers to a situation where most of the representation coefficients of a signal decomposed using an appropriate basis are either zero or can be considered zero, and only a small number of non-zero components are sparsely distributed. However, data from the real world, such as EEG, audio, and images, rarely exhibit sparsity. Therefore, a technique called sparse coding [14] is often employed in image and audio processing. In sparse coding is a method where the input signal is decomposed into the product of a basis matrix and a sparse vector. Let the N-dimensional input signal be denoted as $\mathbf{x} \in \mathbb{R}^{N\times 1}$, the basis matrix as $\boldsymbol{\Psi} \in \mathbb{R}^{N\times P}$, and the sparse vector as $\mathbf{s} \in \mathbb{R}^{P\times 1}$. Applying sparse coding to the input signal $\mathbf{x}$ can be represented as

$$\mathbf{x} = \mathbf{\Psi}\mathbf{s} \tag{1}$$

This enables the application of CS. In this study, we used a discrete cosine transform (DCT) matrix [15] and EEG basis (EEGB) [11] [16] as basis matrices.

B. Signal Compression and Random Under-sampling

In CS, signal compression is performed simultaneously with sampling, enabling low-power signal compression. Signal compression is achieved by multiplying the input signal by the measurement matrix. Let the measurement matrix be $\mathbf{\Phi} \in \mathbb{R}^{M\times N}$ $(M < N)$, then the compressed matrix $\mathbf{y}$ is represented as

$$\mathbf{y} = \mathbf{\Phi}\mathbf{x} \tag{2}$$

Substituting (1) into the above equation yields

$$\mathbf{y} = \mathbf{\Phi}\mathbf{x} = \mathbf{\Phi}\mathbf{\Psi}\mathbf{s}. \tag{3}$$

In conventional CS, Gaussian-distributed measurement matrices, which require significant computational resources, are typically used. However, in this study, we achieved random under-sampling with a measurement matrix that is easier to implement in hardware and is computationally efficient. The matrix was created by setting a randomly determined element in each column of an $M \times N$ zero matrix to one.

C. Reconstruction Algorithm

Let the product of the basis matrix $\mathbf{\Psi}$ and measurement matrix $\mathbf{\Phi}$ be the sensing matrix $\mathbf{\Theta}$, then:

$$\mathbf{y} = \mathbf{\Phi}\mathbf{\Psi}\mathbf{s} = \mathbf{\Theta}\mathbf{s}. \tag{4}$$

As the measurement matrix is known, we can obtain $\mathbf{s}$ by solving (4) during reconstruction, and from (1), we can retrieve the input signal. However, the length of signal $\mathbf{y}$ is shorter than that of signal $\mathbf{s}$, which makes it an underdetermined system, and (4) typically cannot be solved directly. Therefore, we leverage the sparsity of $\mathbf{s}$ and use a method known as a reconstruction algorithm to derive $\mathbf{s}$ from the compressed signal, measurement matrix, and basis matrix. Various reconstruction algorithms have been studied. However, in this study, we employed the block-sparse Bayesian learning (BSBL) algorithm [17], which provides excellent reconstruction accuracy.

D. Chain-generated noise-masking

A CS can be viewed as a form of shared-key encryption if the measurement matrix $\mathbf{\Phi}$ is considered a key. The sender compresses and encrypts the input signal $\mathbf{x}$ using the measurement matrix $\mathbf{\Phi}$, thereby generating a compressed signal $\mathbf{y}$. However, owing to the linear transformation, this method is vulnerable to known-plaintext attacks (KPA) [18]. In response, prior research has proposed a system called chain-generated noise-masking to enhance security. The system adds the pseudo-noise generated using watermarking and chain generation adapted to the CS to the input signal, thereby creating a secure compressed signal.

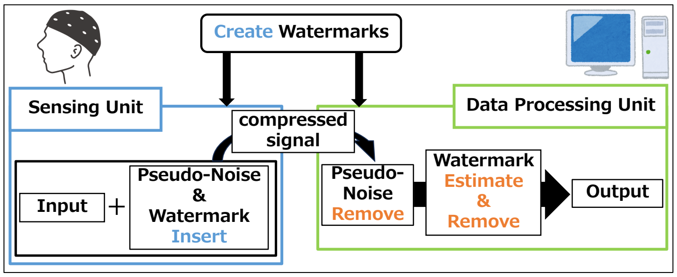

Fig. 1. In the proposed method, a watermark is created in advance, which is shared by the sensing and data processing units. The sensing side generates pseudo-noise using a seed value based on the watermark. The processing side receives a compressed EEG signal that is a combination of the EEG, watermark, and pseudo-noise. The pseudo-noise and watermark can be eliminated by using the pre-shared watermark information.

The specific operation of the chain-generated noise-masking is as follows: First, as shown in the upper part of Fig. 1, several watermark patterns were pre-generated and shared between the transmitter and receiver. Following that, for the transmitter illustrated on the left side of Fig. 1, one of the predefined watermark patterns was selected. Subsequently, a seed value was derived from the selected pattern, which is used to generate a pseudo-noise. As the input signal was sampled and compressed using the measurement matrix, the watermark and generated pseudo-noise were compressed using the same matrix. These signals were then added to the compressed input signal to generate an encrypted compressed signal. On the receiver side, as shown on the right side of Fig. 1, all watermark patterns, the measurement matrix, and seed values are pre-shared. Based on this information, a pseudo-noise was generated and compressed, enabling the receiver to remove the pseudo-noise from the received compressed signal. Upon removing the pseudo-noise, the correlation between the noise-free received signal and stored watermark patterns was examined to identify the watermark selected by the sender. This process also extracts the seed value necessary to generate the pseudo-noise for use in the next step. Finally, the input signal was reconstructed from the received signal after both the pseudo-noise and watermark were removed. By repeating this process continuously, a pseudo-noise is generated in a chain-like manner, thereby ensuring signal security.

E. KPA Scenario

In the KPA scenario, the eavesdropper can reconstruct the measurement matrix $\mathbf{\Phi}$ by accessing pairs of the input signals $\mathbf{x}$ and compressed signal $\mathbf{y}$, denoted as pairs $(\mathbf{x},\mathbf{y})$ [19].

Let the number of such pairs be $\mathbf{p}$, and define $\mathbf{X}_{\text{set}}$ and $\mathbf{Y}_{\text{set}}$ as follows: $\mathbf{X}_{\text{set}}, \mathbf{Y}_{\text{set}}$

$$\begin{aligned} \mathbf{X}_{\text{set}} &= [\mathbf{x}_1 - \mathbf{x}_p] \\ \mathbf{Y}_{\text{set}} &= [\mathbf{y}_1 - \mathbf{y}_p]. \end{aligned} \tag{5}$$

Additionally, let $\phi_{i,j}$ denote the elements in the i-th row and j-th column of the measurement matrix $\mathbf{\Phi}$. The CS equation

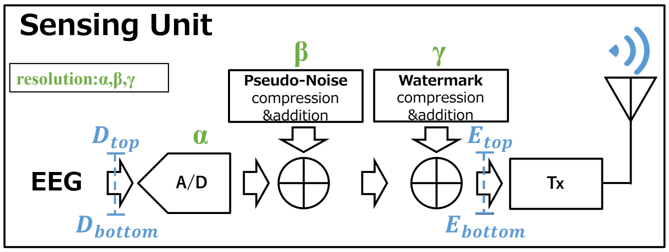

Fig. 2. Schematic of the transmitter. D_{top} and D_{bottom} represent the upper and lower limits of the signal range for the A/D converter, respectively. Similarly, E_{top} and E_{bottom} represent the upper and lower limits of the signal range for the transmitter. α is the resolution of the A/D converter, β is the resolution of the pseudo-noise, and γ is the resolution of the watermark.

can then be written as:

$$\begin{aligned}\mathbf{Y}_{\text{set}} &= \mathbf{\Phi}\mathbf{X}_{\text{set}} \\ &= \begin{pmatrix} \phi_{1,1} & \cdots & \phi_{1,N} \\ \vdots & \ddots & \vdots \\ \phi_{M,1} & \cdots & \phi_{M,N} \end{pmatrix} \mathbf{X}_{\text{set}}.\end{aligned} \tag{6}$$

Therefore, it can be deduced that to determine all the elements $\phi_{i,j}$ of the measurement matrix $\mathbf{\Phi}$, a total of $M \times N$ equations are required. Each pair (X and Y sets) provides M equations. If eavesdropper obtains N pairs of $(\mathbf{X}_{\text{set}}, \mathbf{Y}_{\text{set}})$, then the measurement matrix $\mathbf{\Phi}$ can be completely reconstructed.

III. Transmitter circuit system utilizing chain-generated noise-masking technology

In circuit design, input range and resolution are critical factors when considering power consumption. As shown in the diagram, a transmission circuit that applies the chain-generated noise-masking technique adds watermarking and pseudo-noise to EEG signals. Although this enhances security, increasing the required input range and resolution at the transmitter owing to noise-masking may negate the power-saving advantages of CS. Therefore, in this study, we investigated the design parameters of a transmission circuit system to evaluate their impact on power consumption.

A. Input range

input range refers to the range between the maximum and minimum values of a signal in a measuring device. This range defines the measurable scope; the wider the input range, the more accurately the device measures a broader spectrum of signals. However, a larger input range requires a higher resolution for precise signal reconstruction, which in turn increases the power consumption. This study adopted random under-sampling, a technique that compresses signals by randomly omitting sampling points. Consequently, the input range of the signal remains unchanged even after the A/D conversion. As shown in Fig. 2, the upper and lower limits of the signal range of the A/D converter in the transmission circuit system are denoted by D_{top} and D_{bottom}, respectively. Similarly, the upper limit of the signal range for the transmitter is denoted by E_{top}, where the lower limit is E_{bottom}. When applying masking to a compressed signal, the signal size may increase, potentially requiring a larger input range. However, if there are no problems in the compression and reconstruction processes when $E_{top} - E_{bottom} = D_{top} - D_{bottom}$, the input range does not have to be increased, thus maintaining low-power consumption in the proposed method.

B. Resolution

As shown in Fig. 2, let α represent the resolution of the A/D converter, β the resolution of pseudo-noise, and γ the resolution of the watermark. For example, considering that the resolution of devices such as the Emotiv EPOC X by Emotiv and the B-Alert X series by Advanced Brain Monitoring is 16 bits, if we assume $\alpha = 16$, then if β and γ are at or below the resolution of 16 bits, the overall required resolution of the transmitter can be assumed to be 16 bits. In this case, the insertion of the watermark and noise mask did not increase the required resolution, thereby maintaining low-power consumption.

IV. Evaluation

This study used the CHB-MIT EEG data [20] as the test data to evaluate the stability of transmission and reception, security strength, and reconstruction accuracy based on the aforementioned design methodology. Specifically, we resampled the EEG data from the FP1-FP7 channels of the dataset chb05 from the CHB-MIT database at 200 Hz, excluding the periods of epileptic seizures to focus on using steady-state brain activity, and defined one frame as 6 s. Consequently, 40601 frames of EEG data were obtained. The maximum and minimum data values were measured, and by referencing the larger absolute value of the minimum of $-1379.1\ \mu$V, we set the upper limit of the input range to $E_{top} = 1379.1\ \mu$V and the lower limit to $E_{bottom} = -1379.1\ \mu$V. A quantization program was used to handle data at arbitrary resolutions. The quantization program takes the data to be quantized as full-scale and quantifies both the bit resolution and output data at the given resolution. In addition, as an indicator of the reconstruction accuracy, we used the normalized mean square error (NMSE), defined by the following equation, where $\mathbf{x}$ represents the input signal and $\hat{\mathbf{x}}$ represents the reconstructed signal.

$$\text{NMSE} = \left(\frac{||\hat{\boldsymbol{x}} - \boldsymbol{x}||_2}{||\boldsymbol{x}||_2} \right)^2 . \tag{7}$$

A. Verification of stability of transmission and reception

In the proposed method, the pseudo-noise is generated in a chained manner based on the estimation of the watermark, making it essential for the receiver to reliably estimate the watermark for stable transmission and reception. Therefore, this study specifies the size of the required watermark based on the expected design requirements. In the simulation, eight different watermarks were prepared, and each watermark was added to the EEG data used as the input signal to generate the compressed signal. That is, the watermark was changed eight times for each frame of the input signal. Subsequently, the

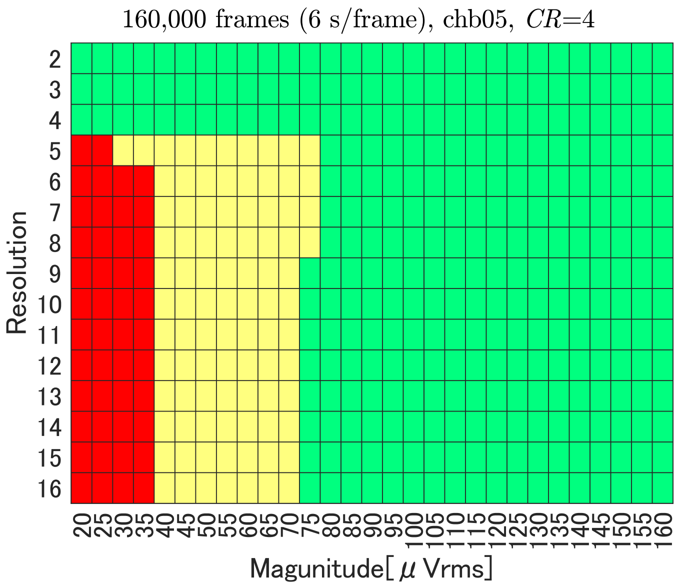

Fig. 3. Shmoo plot showing the magnitude of watermark and estimation accuracy for each resolution. The estimation accuracy is represented by different colors: the red area indicates less than 99.8 %; the yellow area indicates between 99.8 % and less than 100 %; and the green area indicates 100 %.

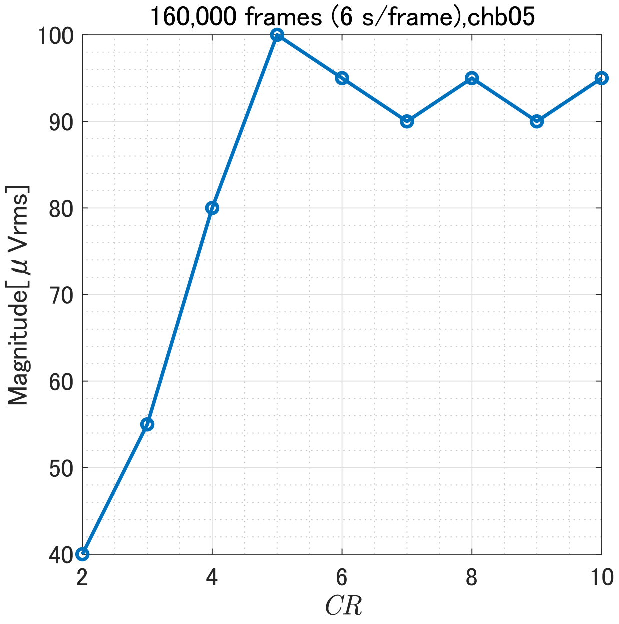

Fig. 4. This figure illustrates the magnitude of the watermark necessary for reliable watermark estimation for each *CR*.

receiver analyzes the correlation between the eight prepared watermarks and the compressed signal to estimate the watermark selected on the transmitter side. The simulations were conducted under the conditions of a compression ratio (*CR*) of 4 and a resolution ranging from 2 to 16 and watermark strengths ranging from 20 to 160 μVrms in 20000×8 sets. The estimation accuracy for each condition was evaluated. The results are presented as a Shmoo plot in Fig. 3, where the horizontal axis represents the watermark strength and the vertical axis represents the resolution. From Fig. 3, it was found that with a resolution of 2 to 4 bits, a reliable estimation could be achieved regardless of the watermark strength. In addition, at a watermark magnitude of 30 to 75 μVrms, the estimation accuracy reaches approximately 99 %, and reliable estimation is ensured at 80 μVrms or higher. Additionally, simulations were conducted with *CR* ranging from 2-10, and Fig. 4 summarizes the required watermark strength for reliable estimation, independent of resolution. As shown in Fig. 4, while the necessary strength increased within the *CR* range of 2-4, it remained between 90 μVrms and 100 μVrms for ratios greater than five. Therefore, a watermark magnitude of 100 μVrms or higher guarantees reliable estimation, regardless of the resolution.

B. Verification of security strength

The proposed method was validated by evaluating the pseudo-noise strength required for sufficient security through the reconstruction accuracy of both the proposed method and eavesdropper, utilizing KPA. The implementation of the KPA employs regularized least squares. The least-squares method minimizes the squared error between predicted and actual values. Regularized least-squares addresses overfitting by adding a regularization parameter λ as follows: Let $\hat{\Phi}$ represent the observation matrix to be estimated, $\mathbf{X}$ represent the input signal, and $\mathbf{Y}$ represent the compressed signal. The matrix $\hat{\Phi}$ can be expressed using the regularization parameter λ in the following equation:

$$\hat{\Phi} = \frac{\mathbf{Y}\mathbf{X}^T}{\mathbf{X}\mathbf{X}^T + \lambda\mathbf{I}} \tag{8}$$

In this study, $\lambda = 0.1$.

Given that the input range of the test data was defined by $E_{top} = 1379.1$ μV and $E_{bottom} = -1379.1$ μV, we hypothesized that as long as the standard deviation σ of the pseudo-noise, representing its strength, does not exceed $1379.1/3 \approx 460$ μV, the noise could be inserted within the allowable input range. In other words, if the inserted noise strength is 460 μV or less, an increase in resolution is not necessary, and there is no additional power consumption owing to the pseudo-noise insertion. In this simulation, the resolutions α, β, and γ are all set to 16 bits. First, we added a watermark with a magnitude of 100 μVrms to the test data, along with the pseudo-noise of arbitrary strengths ranging from 0 to 400 μVrms, and compressed the data at a *CR* of four, following previous studies. Subsequently, both the proposed method and the attacker reconstructed the data, and

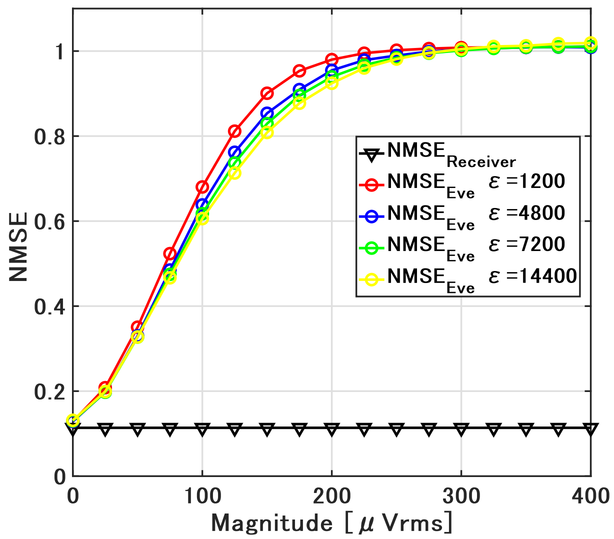

Fig. 5. This graph represents the average NMSE over 1000 frames when the proposed method and eavesdropper attempt to reconstruct brainwave signals with arbitrary pseudo-noise inserted. Here, ϵ indicates the number of pairs of input signals and compressed signals obtained by the attacker.

the NMSE between the reconstructed and original test data was calculated. This compression and reconstruction process was repeated 1000 times for each pseudo-noise strength level, and the results were averaged and plotted in Fig. 5. Here, ϵ represents the number of signal pairs available to the eavesdropper, comprising the input and compressed signals. In Fig. 5, the horizontal axis represents the pseudo-noise strength, and the vertical axis represents the NMSE. The results show that the reconstruction of the receiver accuracy remains constant and accurate, regardless of the noise strength. By contrast, the reconstruction of the eavesdropper accuracy decreased significantly as the pseudo-noise strength increased, with the NMSE gradually converging to one when the noise strength reached 200 μVrms. From these results, we can conclude that a pseudo-noise magnitude of 200 μVrms, which is within the permissible input range, is sufficient to provide adequate security.

C. Verification of resolution dependence of reconstruction accuracy

The resolution required to achieve accurate reconstruction using the proposed method was evaluated. In the simulation, a 100 μVrms watermark and 250 μVrms pseudo-noise were used. These were combined with the test data after quantization at arbitrary resolutions ranging from 4 to 16 bits. Compression and reconstruction processes were then performed, and the NMSE was calculated from the reconstructed data. *CR* values of 4, 6, 8, and 10 were used in this simulation. Additionally, for a *CR* of 10, a simulation was conducted using the EEGB basis matrix, which provides a higher reconstruction accuracy under high compression. Fig.6 shows the results of 10,000 simulations with the average NMSE on the vertical axis and the resolution on the horizontal axis. From these results, it is evident that as the resolution increased from 4 to 6 bits, the reconstruction accuracy improved significantly, followed by a gradual change, and NMSE almost converged at resolutions greater than 10 bits. Moreover, we found that the same results were obtained when the basis matrix was changed.

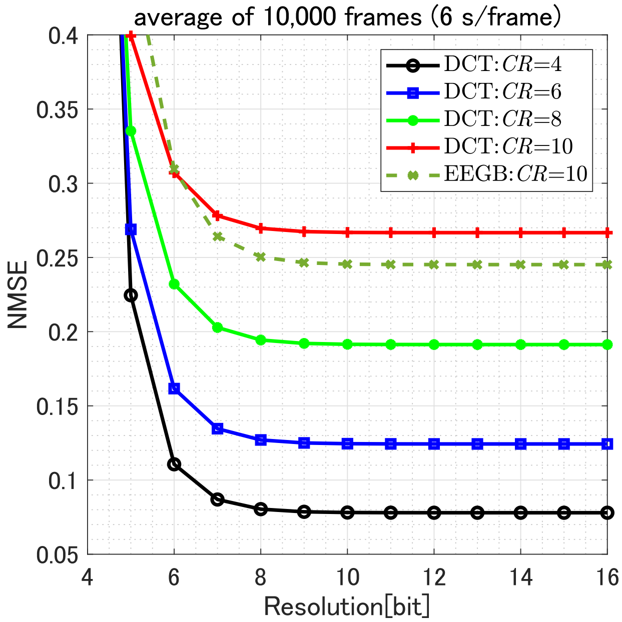

Fig. 6. This graph illustrates the resolution dependence of reconstruction accuracy for various compression ratios when adding a 100 μVrms watermark and 250 μVrms pseudo-noise to the EEG data. The solid line represents data using DCT, while the dashed line represents data using EEGB.

The verification results indicate that when the signal range is set to $E_{top} = 1379.1\ \mu$V and $E_{bottom} = -1379.1\ \mu$V, a watermark with a strength greater than 100 μVrms is required for reliable watermark estimation. Furthermore, a magnitude of 250 μVrms is required to ensure robust security. Even when a noise of this strength is added to the input signal, the resolution does not have to be increased from the perspective of the input range. In addition, a resolution of at least 10 bits is necessary for high-precision recovery. It is also important to consider the potential increase in power consumption due to the noise generation circuit. However, the pseudo-noise generation is performed in a diagnosis domain. Thus, with the future evolution of semiconductor processing technologies, it is expected that the power consumption will continue to scale down compared to the analog circuitry of the transmission system. Therefore, based on the validation results, it can be concluded that the increase in power consumption associated with the proposed system utilizing chain-generated noise-masking techniques is mitigated.

V. CONCLUSION

In this study, we clarified the design guidelines from the perspective of power consumption, focusing on implementation based on security methods proposed in previous studies. Specifically, we examined the security strength with a focus on resolution and input range. The results confirm that when the signal range was set to $E_{top} = 1379.1\ \mu\mathrm{V}$ and $E_{bottom} = -1379.1\ \mu\mathrm{V}$, a watermark magnitude of $100\ \mu\mathrm{Vrms}$ or higher was required for the proposed method to function properly. Additionally, it was found that a noise magnitude of $250\ \mu\mathrm{Vrms}$ is sufficient to ensure security without modifying its input range. Furthermore, it was revealed that a resolution of 10 bits was necessary for a high-precision reconstruction. Based on these findings, we can conclude that the proposed method does not require changes in resolution or input range. Next studies will be conducted using data from multiple subjects, including patients, obtained through wearable devices to evaluate the generalizability and assess inter-subject variability of the proposed method.

ACKNOWLEDGMENT

This work was supported by JSPS Grant-in-Aid for Scientific Research JP24K02914. This work was supported by the JKA Foundation. We acknowledge the support of the ICOM Foundation, Japan, in the form of an International Travel Grant.

REFERENCES

[1] T. Musha, H. Matsuzaki, Y. Kobayashi, Y. Okamoto, M. Tanaka, and T. Asada, "EEG markers for characterizing anomalous activities of cerebral neurons in NAT (Neuronal ActivityTopography) method," *IEEE T BIOMED ENG.*, vol. 60, no. 8, pp. 2332-2338, 2013.

[2] J. Jeong, "EEG dynamics in patients with Alzheimer's diseas," *ClinNeurophysiol*, vol. 115, no. 7, pp. 1490-1505, 2004.

[3] M. Ienca and P. Haselager, "Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity," *Ethics Inf. Technol.*, vol. 18, no. 2, pp. 117-129, 2016.

[4] D. Kanemoto, S. Katsumata, M. Aihara, and M. Ohki, "Compressed sensing framework applying independent component analysis after undersampling for reconstructing electroencephalogram signals," *IEICE Trans. Fundamentals*, vol. E103-A, no. 12, pp. 1647-1654, Dec. 2020.

[5] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289-1306, Apr. 2006.

[6] Y. Okabe, D. Kanemoto, O. Maida, and T. Hirose, "Compressed sensing EEG measurement technique with normally distributed sampling series," *IEICE Trans. Fundamentals*, vol. E105-A,no. 10, pp. 1429-1433, Oct. 2022.

[7] B. Lal, R. Gravina, F. Spagnolo and P. Corsonello, "Compressed sensing approach for physiological signals: a review," *in IEEE Sens. J.*, vol. 23, no. 6, pp. 5513-5534, 15 March15, 2023.

[8] B. Lal, M. H. Conde, P. Corsonello and R. Gravina, "Secure and energy-efficient ECG signal monitoring in the IoT healthcare using compressive sensing," *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2023.

[9] J. Chang, Z. Zhang, Z. Wang, J. Li, L. Meng and P. Lin, "Generative Listener EEG for Speech Emotion Recognition Using Generative Adversarial Networks With Compressed Sensing," *in IEEE J. Biomed. Health Inform.*, vol. 28, no. 4, pp. 2025-2036, Apr. 2024.

[10] K. Mii, D. Kanemoto, O. Maida, and T. Hirose, "0.36μw/channel capacitively-coupled chopper instrumentation amplifier in EEG recording wearable devices for compressed sensing framework," *Jpn. J. Appl. Phys.*, vol. 63, 03SP54, 2024.

[11] R. Matsubara, D. Kanemoto, O. Maida, and T. Hirose, "Reducing power consumption in LNA by utilizing EEG signals as basis matrix in compressed sensing," *in Proc. IEEE Int. Symp. Circuits Syst.*, (ISCAS), May. 2024, pp. 1-5.

[12] T. Miyata, D. Kanemoto, O. Maida, and T. Hirose, "Random undersampling wireless EEG measurement device using a small TEG," *in Proc. IEEE Int. Symp. Circuits Syst.*, (ISCAS), May. 2023, pp.1-5.

[13] R. Tsunaga, D. Kanemoto, O. Maida, and T. Hirose, "Noise-maskingcryptosystem using watermark and chain generation for EEG-measurement with compressed sensing," *in Proc. IEEE Int. Conf. Consum. Electron.*, (ICCE), Jan. 2024, pp. 1-6.

[14] K. Nagai, D. Kanemoto, and M. Ohki, "Applying K-SVD dictionary learning for EEG compressed sensing framework with outlier detection and independent component analysis," *IEICE Trans. Fundamentals*, vol. E104-A, no. 09, pp. 1375-1378, Sep. 2021.

[15] Z. Zhang, T. -P. Jung, S. Makeig, B. D. Rao, "Compressed sensing of EEG for wireless telemonitoring with low energy consumption and inexpensive hardware," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 1, pp. 221-224, Jan. 2013.

[16] D. Kanemoto, and T. Hirose, "EEG measurements with compressed sensing utilizing EEG signals as the basis matrix," *in Proc. IEEE Int. Symp. Circuits Syst.*, (ISCAS), May. 2023, pp.1-5.

[17] Z. Zhang and B. D. Rao, "Extension of SBL algorithms for the recovery of block sparse signals with intra-block correlation," *IEEE Trans. Signal Process.*, vol. 61, no. 8, pp. 2009-2015, Apr. 2013.

[18] V. Cambarei, M. Mangia, F. Paresschi, R. Rovatti, and G. Setti, "On known plaintext attacks to a compressed sensing-based encryption: A quantitative analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2182-2195, 2015.

[19] T. -S. Chen, K. -N. Hou, W. -K. Beh, and A. -Y. Wu, "Low-complexity compressed-sensing-based watermark cryptosystem and circuits implementation for wireless sensor networks," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 27, no. 11, pp. 2485-2497, 2019.

[20] A. H. Shoeb, "Application of machine learning to epileptic seizure onset detection and treatment," *Massachusetts Institute of Technology*, PhD 2009.