A Data Concealing Technique with Random Noise Disturbance and a Restoring Technique for the Concealed Data by Stochastic Process Estimation

Tomohiro Fujii and Masao Hirokawa

Abstract We propose a technique to conceal data on a physical layer by disturbing them with some random noises, and moreover, a technique to restore the concealed data to the original ones by using the stochastic process estimation. Our concealing-restoring system manages the data on the physical layer from the data link layer. In addition to these proposals, we show the simulation result and some applications of our concealing-restoring technique.

Keywords Concealing-restoring system · OSI · Physical layer · Data link layer · Noise-disturbance · Stochastic process estimation · Noise-filtering · Kalman filter · Particle filter

1 Introduction

Micro-device technology in the near future realizes the remote control of microprocessor chips in several things such as household electric appliances, information-processing equipment, and even brain–computer/brain–machine interfaces from the outside through wireless communications or the so-called IoT (i.e., Internet of Things). Moreover, it enables the automatic operation of such things with the remote control. They are going to infiltrate society and play several important roles in every area of society. We then have to establish the data security for them (Youm 2017; Román-Castro et al. 2018; Lin et al. 2018; Clausen et al. 2017). In particular, we have to stem the hacking of the remote control and the wiretapping of the data of communication. We are interested in a data concealing technique with disturbance on a physical layer and a restoring technique for those concealed data. Here, the

T. Fujii (✉) · M. Hirokawa (✉)
Graduate School of Engineering, Hiroshima University, Hiroshima, Japan
e-mail: fujii@amath.hiroshima-u.ac.jp

M. Hirokawa
Graduate School of ISEE, Kyushu University, Fukuoka, Japan
e-mail: hirokawa@inf.kyushu-u.ac.jp

T. Takagi et al. (eds.), *International Symposium on Mathematics, Quantum Theory, and Cryptography*, Mathematics for Industry 33,
https://doi.org/10.1007/978-981-15-5191-8_11

physical layer is the lowest layer of the open systems interconnection (OSI) (Kain and Agrawala 1992) (see Fig. 1). OSI is a reference model to grasp and analyze how data are sent and received over a computation or communication network. Some methods using disturbance have been presented to conceal data for storage and communication. For instance, chaotic cryptology (Cuomo and Oppenheim 1993; Grassi and Mascolo 1999; Lenug and Lam 1997; Wu and Chua 1993) uses chaos to make the disturbance. The method using cryptographic hash functions for the disturbance has lately been gaining a practical position (Merkle 1979, 1989; Damgård 1989; Schneier 2015). There have been some endeavors for the concealing technique on physical layers: the chaos multiple-input multiple-output (Okamoto and Iwanami 2006; Zheng 2009; Okamoto 2011; Okamoto and Inaba 2015; Ito et al. 2019). Meanwhile, it is noteworthy that the secured telecommunication using noises has been actively studied (Wyner 1975; Hero 2003; Goel and Negi 2008; Swindlehurst 2009; Mukherjee and Swindlehurst 2011). In that technique, we send some noises from interference antennas to the signal on a carrier wave sent from an antenna; we have the signal interfering with the noises and make it an interference wave. There, however, may be a way to remove the noises from the interference wave and to wiretap the original signal (Ohno et al. 2012).

We take interest in how to conceal data on a physical layer using some random noise disturbances and how to restore those concealed data applying a stochastic filtering theory to maintain the safety of data over a proper period of time, which is different from the interference wave method. Thus, our concealing-restoring system should be installed on a data link layer above the physical layer (see Fig. 1). Although we employ the disturbance by random noises instead of the chaotic one, we can design our concealing-restoring system so that it includes the chaotic disturbance (Fujii and Hirokawa 2020). The idea of the concealing-restoring system was primarily originated in keeping security for the data processed on the physical layer of our developing quantum-sensing equipment over a necessary period. This equipment detects and handles some ultimate personal information. Since we must remove several noises on the physical layer in any case, we make our concealing-restoring system coexist with the denoising system of the equipment. We then consider the information concealing method for qubits (i.e., quantum bits) using the random noises in classical physics. The qubits $|0\rangle$ and $|1\rangle$ are represented by spin states $|\uparrow\rangle$ and $|\downarrow\rangle$, namely, $|0\rangle = |\uparrow\rangle = (1, 0)$ and $|1\rangle = |\downarrow\rangle = (0, 1)$. A general qubit $|q\rangle$ can be described with the superposition of the qubits $|0\rangle$ and $|1\rangle$: $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ for some complex numbers α and β with $|\alpha|^2 + |\beta|^2 = 1$. Thus, the qubit can have the representation, $|q\rangle = (\Re\alpha, \Im\alpha, \Re\beta, \Im\beta)$, and an information sequence of qubits, $|q_1\rangle, |q_2\rangle, \ldots, |q_\nu\rangle$, is expressed with a finite sequence,

$$\Re\alpha_1 \ \Im\alpha_1 \ \Re\beta_1 \ \Im\beta_1 \ \Re\alpha_2 \ \Im\alpha_2 \ \Re\beta_2 \ \Im\beta_2 \ \ldots \ \Re\alpha_\nu \ \Im\alpha_\nu \ \Re\beta_\nu \ \Im\beta_\nu.$$

We transform it into an electrical signal X_t, $0 \le t \le 4\nu$, using linear interpolation. We process the electrical signal in a microprocessor, made by some semiconductors, of our quantum-sensing equipment. Since the microprocessor is for the conventional computation (i.e., not quantum computation), we need to transport the electrical

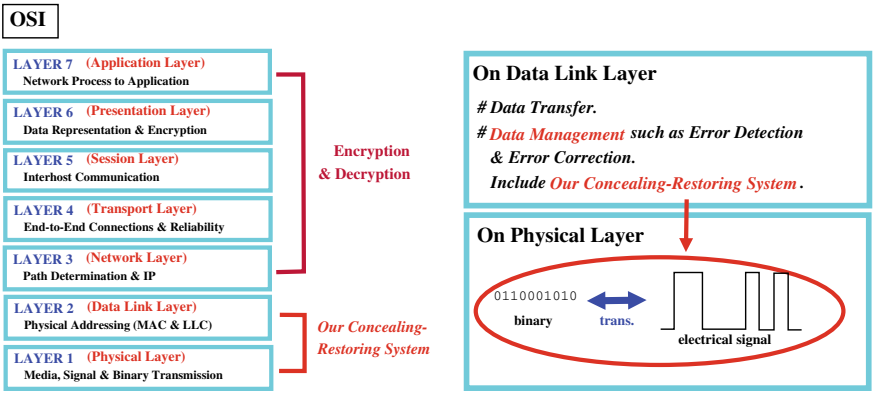

Fig. 1 The left picture shows that the OSI consists of 7 layers. The encryption and decryption are usually done on one out of layers between Layer 3 and Layer 7, typically on the presentation layer. The right picture shows what we aim our concealing-restoring system at

signal to memory or register according to a microarchitecture. To keep the security for the electric signal X_t while processing, storing, and saving it, we employ a mathematical idea to conceal it using the noise disturbance. In this paper, we introduce that mathematical idea for more general signals on the physical layer and more broad applications.

As some applications derive therefrom, we first establish a mathematical technique for concealing data by the disturbance with randomness of the noises, and moreover, a mathematical technique for restoring the concealed data by the stochastic process estimation. In addition to these establishments, we show the simulation result and some applications for the two techniques. The idea of our method to conceal data comes from an image of the scene when we conceal a treasure map, and it is so simple as follows:

(c1) we plaster over the treasure map at random and make it messy;
(c2) we repeat c1 and plaster it over repeatedly.

In this paper, we mathematically realize c1 and c2, and make their implementation on conventional computers. In addition to c1 and c2, we can consider that

(c3) we tear the muddled map by c1 and c2, and split it into several pieces, though we do not make its implementation in this paper.

We are planning that we use the concealed data for saving them in memory or for sending them for telecommunication. We expect to use our methods in the situation where the physical layer is under restrictions in the implementation space due to a small consumed electric power, a small arithmetic capacity, a small line capacity, and a bad access environment. Concretely, we hope to apply the implementation of our techniques to the remote control of drones and devices on them, and to the security of some data sent from those devices. Moreover, we suppose the situation where it is too harsh to make a remote maintenance of the physical layer, for example, in outerspace development or seafloor development.

2 Mathematical Setups

We first explain the outline of how to make our concealing-restoring system for data X_t, $t \in \mathbb{R}$. The concealing-restoring system is given by a simultaneous equation system (SES). This SES consists of some stochastic differential equations (SDEs), linear equations, and a nonlinear equation (NLE). The data X_t is input as the initial data of the SES. We prepare N functionals F_i, $i = 1, 2, \ldots, N$, making the SDEs. We suppose that each form of the individual functional F_i is known only by those who conceal the original data X_t and restore the concealed data. We use the forms of the functionals as well as the composition of the SES for secret keys or common keys. We prepare $2N$ random noises $W_t^{j,i}$, $j = 1, 2$; $i = 1, 2, \ldots, N$, for the SDEs, and a nonlinear bijection f for the NLE. The SDEs for processes X_t^i, $i = 1, 2, \ldots, N$, and the NLE for the process X_t^{N+1} are used to introduce the noise disturbance in our concealing-restoring system. We also use the means, variances, and distributions of the random noises as well as the nonlinear bijection as secret keys. As shown below, we obtain $N + 1$ concealed data, U_t^i, $i = 1, 2, \ldots, N, N + 1$, using the SDEs and the NLE. We use them as the data for saving in a digital memory such as a semiconductor memory or an analog memory such as a magnetic tape. We may also put the concealed data on a carrier wave and send them. This is the outline of the data concealing. Meanwhile, the data restoration is done in the following. Using the stochastic filtering theory and the inverse function f^{-1}, we remove the random noises from every concealed data U_t^i, and we estimate the process X_t^i. We denote the estimate by $\widehat{X}_t^i$, and call it *estimated data* for the process X_t^i. We regard the estimate $\widehat{X}_t^1$ as the *restoration* of the original data X_t. We denote it by $\widehat{X}_t$.

We here explain how to make the data X_t from binary data. We use the low/high-signal for the binary data in this paper though there are many other ways. Thus, we represent 'low' by 0 and 'high' by 1. For $n + 1$ bits, $a_0, a_1, \ldots, a_n \in \{0, 1\}$, we concatenate them and make a word $a_0 a_1 \ldots a_n$. We employ the following linear interpolation as a simple digital–analog (D/A) transformation. We first define X_i by

$$X_i = \begin{cases} +1 & \text{if } a_i = 1, \\ -1 & \text{if } a_i = 0, \end{cases} \qquad i = 0, 1, \ldots, n.$$

We connect X_i and X_{i+1} with a straight line for each $i = 0, 1, \ldots, n-1$, and we have a polygonal line X_t, $0 \le t \le n$. When the data X_t are made from the binary word $a_0 a_1 \ldots a_n$, we call X_t a *binary pulse* for the word $a_0 a_1 \ldots a_n$. As for the restoration of the word, we use the simple analog–digital (A/D) transformation to seek the character $\widehat{a}_i \in \{0, 1\}$ for each $i = 0, 1, \ldots, n$, and make a word $\widehat{a}_0 \widehat{a}_1 \ldots \widehat{a}_n$ for the original word $a_0 a_1 \ldots a_n$ in the following. We determine a threshold in advance between those who conceal the binary pulse and restore its concealed data to it. The threshold is basically determined taking into account the mean and variance of the random noises when used for concealing data. For each $i = 0, 1, \ldots, n$, we define the character $\widehat{a}_i$ by

$$\widehat{a}_i = \begin{cases} 1 & \text{if } \widehat{X}_i > \text{threshold}, \\ 0 & \text{if } \widehat{X}_i \le \text{threshold}. \end{cases}$$

We call the word $\widehat{a}_0\widehat{a}_1 \dots \widehat{a}_n$ *restored word* from $\widehat{X}_t$. We note that the mean and the variance play important roles to define a threshold between 'low' and 'high' of signals, in particular, when we use ν-adic numbers such as octal numbers and hexadecimal numbers instead of binary numbers.

From now on, we explain mathematical details for our data concealing technique and restoring technique. We give our secret SES by

$$F_i(X_t^i, \dot{X}_t^i, U_t^i, W_t^{1,i}) = 0, \qquad i = 1, 2, \dots, N, \tag{1}$$

$$X_t^{i+1} = c^i X_t^i + W_t^{2,i}, \qquad i = 1, 2, \dots, N, \tag{2}$$

$$U_t^{N+1} = f\left(X_t^{N+1}\right). \tag{3}$$

In the above system, $\dot{X}_t^i$ stands for the time derivative dX_t^i/dt of the process X_t^i, and c^i is a constant. The initial data X_t^1 is given by $X_t^1 = X_t$. The concealed data U_t^i, $i = 1, 2, \dots, N, N+1$, are directly defined by Eqs. (1) and (3), not Eq. (2). That is, we can hide the linear part of our system because we do not have to make an interference wave. This is the point of our method that is different from that of telecommunication using noises (Wyner 1975; Hero 2003; Goel and Negi 2008; Swindlehurst 2009; Mukherjee and Swindlehurst 2011). Introducing functionals, G_i, $i = 1, 2, \dots, N$, and using them for Eq. (2), we can introduce the chaotic disturbance in our concealing-restoring system (Fujii and Hirokawa 2020).

Equations (1) and (3) are the mathematical realization of c1. The repetition of Eq. (1) from $i = 1$ to $i = N$ with the help of Eq. (2) is for the realization of c2. We can mathematically realize c3 as follows: Take numbers r_ℓ, $\ell = 1, 2, \dots, M$, with $\sum_{\ell=1}^M r_\ell = 0$, and define

$$U_t^\ell = \frac{1}{M}\left(U_t^i + r_\ell U_t^j\right), \quad \ell = 1, 2, \dots, M,$$

where $i \neq j$. Then, we can split the data U_t^i into the data U_t^ℓ, $\ell = 1, 2, \dots, M$. In the case $M = 2$, for instance, we generate a random number r with $r \neq 0$, and set r_1 and r_2 as $r_1 = r$ and $r_2 = -r$. From the split data, U_t^ℓ, $\ell = 1, 2, \dots, M$, we can restore the data U_t^ℓ to the data U_t^i and U_t^j by

$$U_t^i = \sum_{\ell=1}^M U_t^\ell \qquad \text{and} \qquad U_t^j = r_\ell^{-1}\left(M U_t^\ell - U_t^i\right)$$

for an ℓ satisfying $r_\ell \neq 0$. We can also use the sequence, $r_1, r_2, \dots, r_M$, as a secret or common key.

We note that the last stochastic process appearing in Eq. (3) has the form,

$$X_t^{N+1} = c^1 \cdots c^N X_t + \sum_{i=1}^{N-1}\left(\prod_{j=i+1}^N c^j\right) W_t^{2,i} + W_t^{2,N}. \tag{4}$$

2.1 How to Conceal Data

We take the original data X_t as initial data,

$$X_t^1 = X_t.$$

Inputting it into Eq. (1) with the noise $W_t^{1,1}$, we conceal it by the SDE,

$$F_1(X_t^1, \dot{X}_t^1, U_t^1, W_t^{1,1}) = 0.$$

We seek U_t^1 in the above and obtain a concealed data U_t^1. By Eq. (2),

$$X_t^2 = c^1 X_t^1 + W_t^{2,1},$$

we have data X_t^2 for the next step. These data X_t^2 consist of the superposition (i.e., linear combination) of X_t^1 and $W_t^{2,1}$, and thus, there is a possibility that a wiretapper removes the noise $W_t^{2,1}$ and wiretap X_t^1. Thus, to improve the security with another noise-disturbance, we have the same procedure again. We input the data X_t^2 into Eq. (1) with the noise $W_t^{1,2}$,

$$F_2(X_t^2, \dot{X}_t^2, U_t^2, W_t^{1,2}) = 0.$$

We then obtain the concealed data U_t^2. Repeating the same procedures, we obtain the concealed data, $U_t^1, U_t^2, \ldots, U_t^N$, and hide the data, $X_t^1, X_t^2, \ldots, X_t^N$.

At last, input the concealed data X_t^N into Eq. (2) and get the data X_t^{N+1}. We input this into Eq. (3) and hide it. We then obtain the last concealed data U_t^{N+1}. In this way, the sequence of the concealed data, $U_t^1, U_t^2, \ldots, U_t^N, U_t^{N+1}$, is created.

In the case where the original data are digital, and they give the binary pulse X_t, the concealed data, U_t^i, $i = 1, 2, \ldots, N, N+1$, merely become analog data. So, a wiretapper has to know A/D transformation to obtain the original digital data as getting the concealed data. Therefore, the D/A and A/D transformations play an important role for the concealing-restoring system for some digital data. We can also use them as secret or common keys.

2.2 How to Restore Data

Since the nonlinear function f is bijective, we can restore the concealed data U_t^{N+1} to the data X_t^{N+1} by

$$X_t^{N+1} = f^{-1}\left(U_t^{N+1}\right).$$

In the light of the stochastic filtering theory, Eqs. (1) and (2) are the state equation and the observation equation, respectively, and they make the system of the noise-

filtering. Inputting the above X_t^{N+1} into Eq. (2), and the concealed data U_t^N into Eq. (1), we have simultaneous equations to seek the data X_t^N,

$$F_N(X_t^N, \dot{X}_t^N, U_t^N, W_t^{1,N}) = 0,$$
$$X_t^{N+1} = c^N X_t^N + W_t^{2,N}.$$

Since we cannot completely restore the noises to the original ones, $W_t^{1,N}$ and $W_t^{2,N}$, we cannot completely seek the stochastic process X_t^N. Thus, we estimate it with the help of a proper stochastic filtering theory to remove the random noises. We then obtain the estimated data $\widehat{X}_t^N$.

Inputting the estimated data $\widehat{X}_t^N$ into the slot of X_t^N of Eq. (2), and the concealed data U_t^{N-1} into Eq. (1), we reach simultaneous equations to seek the data X_t^{N-1},

$$F_{N-1}(X_t^{N-1}, \dot{X}_t^{N-1}, U_t^{N-1}, W_t^{1,N-1}) = 0,$$
$$\widehat{X}_t^N = c^{N-1} X_t^{N-1} + W_t^{2,N-1}.$$

In the same way as in the above, the stochastic filtering theory gives us the next estimated data $\widehat{X}_t^{N-1}$. We repeat this procedure, and obtain the estimated data, $\widehat{X}_t^N, \widehat{X}_t^{N-1}, \ldots, \widehat{X}_t^2, \widehat{X}_t^1$, by turns, and we pick up the last estimate $\widehat{X}_t^1$. This is the restoration $\widehat{X}_t$ of the original data X_t.

3 Example of Functionals and Simulation

As for how to determine each functional, F_i, $i = 1, 2, \ldots, N$, any definition of it is fine so long as a noise-filtering theory is established for the system with F_i. To restore the concealed data, $U_t^1, U_t^2, \ldots, U_t^N, U_t^{N+1}$, generally speaking, we have to know the concrete forms of the functionals, and the noise-filtering theory. Therefore, we must hide both for securing the original data. In this paper, however, we disclose one of examples of the concrete definition of the functionals and one of examples of the noise-filterings, which should actually be supposed to be in secret. We point out that the example of concealing-restoring system introduced in this section is not valid for other functionals. In particular, it is not tolerant of nonlinearity. See Sect. 5.

3.1 An Example of the Set of Functionals

We release an example of functionals in this section. We determine functions $A^i(t)$, $v^i(t)$, and non-zero constants b_u^i, b^i in secret. Here $v^i(t)$ can be a random noise. For instance, we often make $v^i(t)$ by the linear interpolation based on normal random numbers. Namely, we first assign a normal random number with $N(0, \sigma_v^2)$ to $v^i(k)$ for each i and k, and then, connect them by linear interpolation. Here, $N(0, \sigma_v^2)$

means the normal distribution whose mean and standard deviation are, respectively, 0 and σ_v. We give each functional F_i such that it makes a SDE,

$$dX_t^i = \left(A^i(t) - 1\right) X_t^i dt + b_u^i U_t^i dt + b^i v^i(t) dt - b_u^i dB_t^i, \tag{5}$$

for $i = 1, 2, \ldots, N$. That is,

$$\dot{X}_t^i = \left(A^i(t) - 1\right) X_t^i + b_u^i U_t^i + b^i v^i(t) - b_u^i W_t^{1,i}. \tag{6}$$

Here, $W_t^{1,i}$ and $W_t^{2,i}$ are Gaussian white noises whose mean $m^{j,i}$ and variance $V^{j,i}$ are, respectively, 0 and $(\sigma_j^i)^2$. B_t^i is the Brownian motion given by $W_t^{1,i} = dB_t^i/dt$, $i = 1, 2, \ldots, N$. We assume that the noises $W_t^{1,i}$ and $W_t^{2,i}$ are independent for each $i = 1, 2, \ldots, N$, but the noises $W_t^{2,i}$, $i = 1, 2, \ldots, N$, are not always independent. Thus, in the case where they are not independent, the linear combination of white noises appearing in Eq. (4) is not always white noise.

We regard the functions $A^i(t)$, the constants b_u^i, b^i, and the mean $m^{j,i}$ and variance $V^{j,i} = (\sigma_j^i)^2$ of the white noises as secret keys which are known only by the administrator of our concealing-restoring system. We use functions $v^i(t)$ as common keys. Since Eqs. (5) and (2), respectively, play the individual roles of the state equation and observation equation in the stochastic filtering theory, we employ the linear Kalman filtering theory (Kalman 1960; Kallianpur 1980; Bain and Crisan 2009; Grewal and Andrews 2015) to obtain the restoration $\widehat{X}_t$.

Using Eq. (6) we give the concealed data U_t^i, $i = 1, 2, \ldots, N$, by

$$U_t^i = \frac{1}{b_u^i}\left\{dX_t^i + \left(1 - A^i(t)\right) X_t^i - b^i v^i(t)\right\} + dB_t^i. \tag{7}$$

In addition to these concealed data, we give the last concealed data U_t^{N+1} by Eq. (3). Conversely, since we obtain the data X_t^{N+1} by $X_t^{N+1} = f^{-1}(U_t^{N+1})$, we can estimate the data, X_t^N, X_t^{N-1}, …, X_t^1, from the concealed data, U_t^N, U_t^{N-1}, …, U_t^1, using the linear Kalman filtering theory.

3.2 *Simulation of Concealing and Restoring Data on Physical Layer*

In our simulation of concealing and restoring data on the physical layer, we employ the message digest (Rivest 1991, 1992a, b; Suhaili and Watanabe 2017; MessageDigest 2020) to check the coincidence of the original word $a_0 a_1 \ldots a_n$ and its restored word $\widehat{a}_0 \widehat{a}_1 \ldots \widehat{a}_n$ though the message digest works on upper layers. Moreover, we can use the message digest to detect any falsification of the concealed data. We take the original word $a_0 a_1 \ldots a_n$ as a message, and then, produce its digest. We also produce the digest for the restored word $\widehat{a}_0 \widehat{a}_1 \ldots \widehat{a}_n$. Comparing hash values of the

two digests, we can make the check of the coincidence and the detection of the falsification at the same time. The check and detection should be performed on a layer out of layers between Layer 3 and Layer 7. In our simulation, we employ SHA-256 to make the hash values (Secure Hash Standard 2015).

To make the estimation in the simulation, we employ the linear Kalman filtering theory under the following conditions. We make Eqs. (1)–(3) for $N = 2$ with $A^i(t) = 0.1$ (constant function), $b^i = 1$, $b^i_u = 1$, and $c^i = 1$ for each $i = 1, 2$. We define the common key $v^i(t)$ by the linear interpolation based on a normal random number with $N(0, 1^2)$. We assume that the means of white noises are all 0. The standard deviation of the white noise $W_t^{j,1}$ is $\sigma_j^1 = 0.1$, and that of the white noise $W_t^{j,2}$ is $\sigma_j^2 = 1$. The length of the word $a_0 a_1 \ldots a_n$ is 100, and therefore, $n = 99$.

Our original word $a_1 a_2 \ldots a_{99}$ is given by Eq. (8). We here note that we remove the character a_0 because we cannot estimate the first bit in our concealing-restoring system.

$$\begin{aligned} &0000110010011100100010000010111011111111001000110 \\ &10100111101111011001010101000101101111001101110 01. \end{aligned} \tag{8}$$

Then, we get its binary pulse X_t as in Fig. 2. The hash value of the digest made from the original word (8) is

$$979bca61579e002c9097c78088740e9fdaf21535d6a5c5876bd8623a86185292. \tag{9}$$

We make the concealed data, U_t^1 and U_t^2, by Eq. (7) with the help of the linear equation given in Eq. (2). We finally make the concealed data U_t^3 using the nonlinear equation given in Eq. (3) with $f(\xi) = \xi^3$. Their graphs are in Figs. 3 and 4. Following the Kalman filtering theory, we remove the white noises, and estimate the binary pulse X_t. Then, we obtain the restoration $\widehat{X}_t$ as in Fig. 5. The concrete algorithm to seek the restoration $\widehat{X}_t$ comes out in Ref. Fujii and Hirokawa (2020). Let us take 0 as the

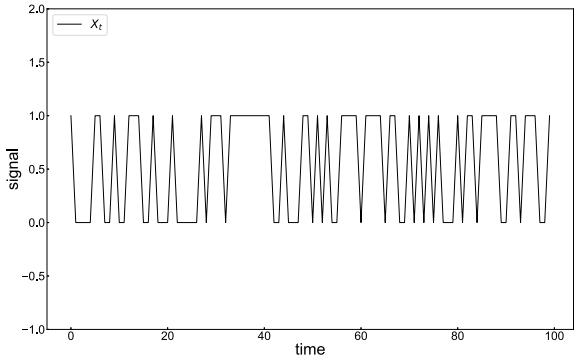

Fig. 2 The binary pulse X_t transformed from the original word (8)

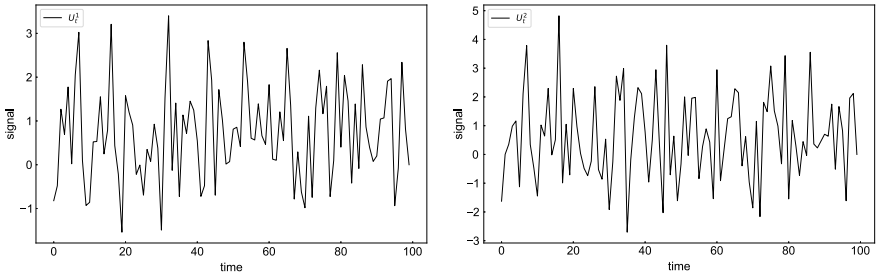

Fig. 3 The concealed data, U_t^1 (left) and U_t^2 (right), for the binary pulse X_t in Fig. 2

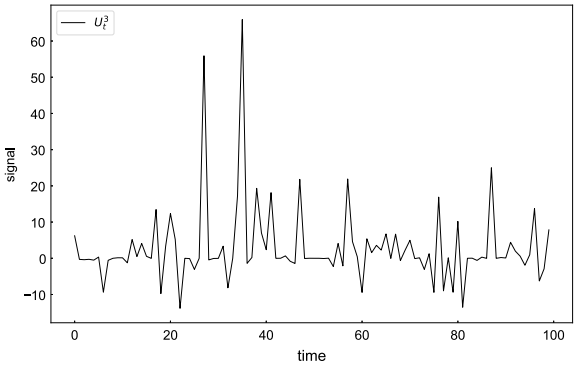

Fig. 4 The concealed data U_t^3 for the binary pulse X_t in Fig. 2

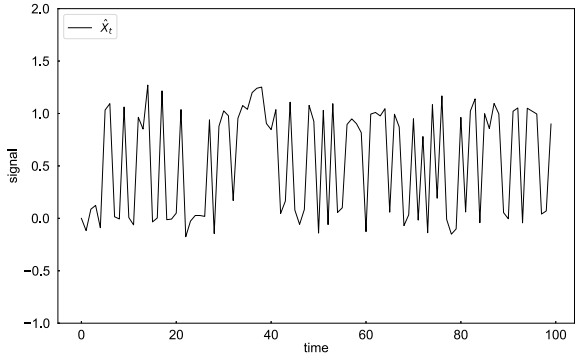

Fig. 5 The restoration $\widehat{X}_t$ for the binary pulse X_t in Fig. 2

threshold. Then, we obtain the restored word $\widehat{a}_1\widehat{a}_2\ldots\widehat{a}_{99}$ and the hash value of its digest made from the restoration $\widehat{X}_t$. We can achieve positive results that they are the same as Eqs. (8) and (9), respectively.

We note that the graphs in Figs. 3 and 4 say that the concealed data, U_t^1, U_t^2, and U_t^3, are merely analog data. If a wiretapper becomes aware that the concealed data are for digital ones and knows our A/D transformation in some way, then the wiretapper gets a binary word from the concealed data as follows:

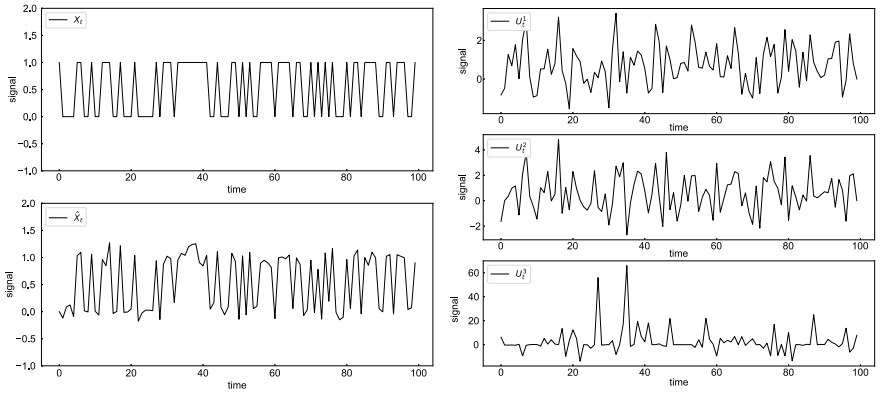

Fig. 6 X_t (Fig. 2) and $\widehat{X}_t$ (Fig. 5) from the above of the left 2 graphs. U_t^1 (Fig. 3), U_t^2 (Fig. 3), and U_t^3 (Fig. 4) from the above of the right 3 graphs. Here $t \in [0, 99]$

$$0011101100011101100011100000100110101111100110110 0$$
$$1101111110100111100001011110010110101100011110011 0$$

for U_t^1,

$$0001101100011101101011000010010011100111011001010$$
$$0101100100100111101001011111010100001000111011011 0$$

for U_t^2, and

$$1000000000001011010111000001000100110011110010010 0$$
$$0000010110011111010110001010001000000100011101100 1$$

for U_t^3. Here, since the wiretapper does not know that we removed the first bit, every concealed data U_t^i makes the word consisting of 100 characters.

In Fig. 6 we show the comparison of the original binary pulse X_t, its restoration $\widehat{X}_t$, and the concealed data U_t^i, $i = 1, 2, 3$.

4 Application to Data on Physical Layer and Presentation Layer

4.1 Binary Data of Pictorial Image

We now apply the technology of our mathematical method to the binary data of a pictorial image. We use digital data of a pictorial image in the ORL Database of

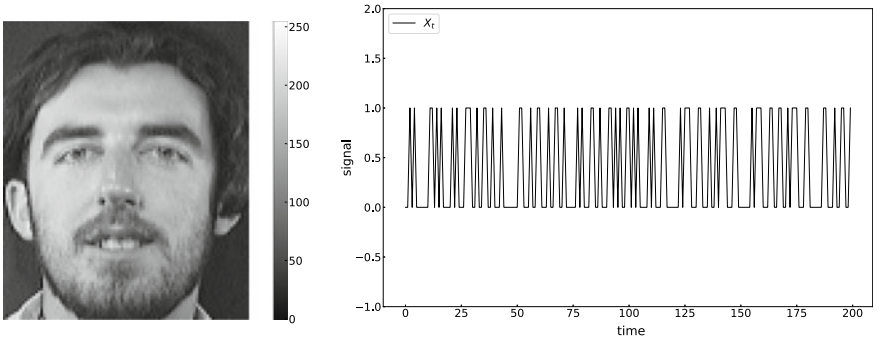

Fig. 7 The original pictorial image (left) with the digital data, and its binary pulse X_t (right) only for $t \in [0, 200]$

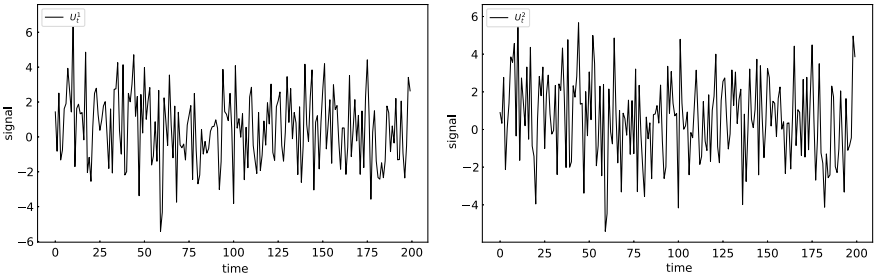

Fig. 8 The concealed data, U_t^1 (left) and U_t^2 (right), for the binary pulse X_t in Fig. 7. Here $t \in [0, 200]$ only

Faces, an archive of AT&T Laboratories Cambridge (The ORL Database of Faces 2020). The data have the grayscale value of 256 gradations (8bit/pixel). We set our parameters as $A = A^i = 0.1, b = b^i = 1, b_u = b_u^i = 1, c = c^i = 1, \sigma_1 = \sigma_1^i = 0.1$, and $\sigma_2 = \sigma_2^i = 1$. We determine the common key $v^i(t)$ in the same way as in Sect. 3.2 with $\sigma_v = 2$. The original pictorial image and its binary pulse X_t are obtained as in Fig. 7. Here, the upper bound of t is $92 \times 112 = 10304$ and t runs over $[0, 10304]$. We obtain the concealed data, U_t^1 and U_t^2, by Eq. (7) as in Fig. 8, and the concealed data U_t^3 by Eq. (3) as in Fig. 9. The restoration $\widehat{X}_t$ and the restored pictorial image from it are in Fig. 10.

If a wiretapper tries to get the original pictorial image from the concealed data $U_t^i, i = 1, 2, 3$, since the concealed data are analog as in Figs. 8 and 9, the wiretapper has to know our A/D transformation, and our transformation from the digital data to a pictorial image as well as some keys used in SES. The latter transformation should be done on upper layers. We now assume that the wiretapper can know the transformations. Then, each pictorial image of the concealed data, $U_t^i, i = 1, 2, 3$, is in Fig. 11. The format of the pictorial image of Fig. 7 is PGM (i.e., portable gray map). In fact, we cannot restore the PGM header from the concealed data, that is, the header of the PGM is completely broken. Thus, the wiretapper has to realize that

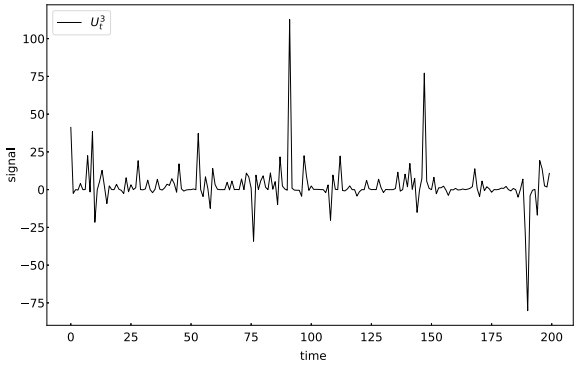

Fig. 9 The concealed data U_t^3 for the binary pulse X_t in Fig. 7. Here $t \in [0, 200]$ only

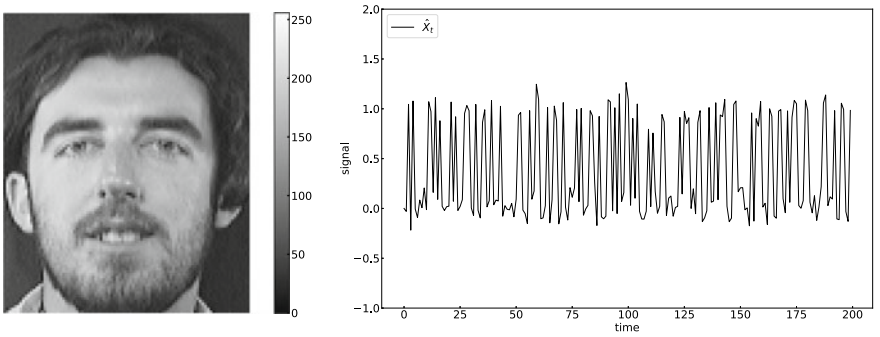

Fig. 10 The restoration $\widehat{X}_t$ for the binary pulse X_t in Fig. 7 only for $t \in [0, 200]$ (right) and the restored pictorial image (left) of $\widehat{X}_t$

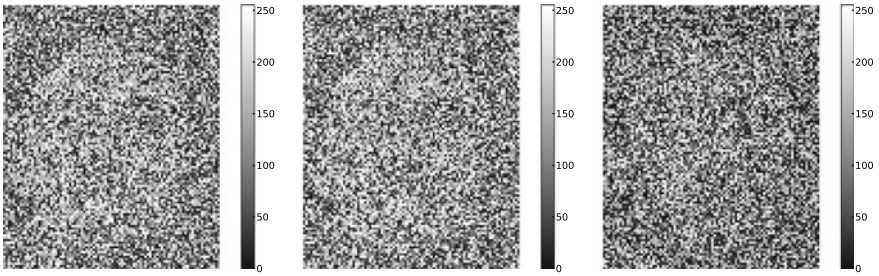

Fig. 11 From the left, pictorial images of the concealed data, U_t^1, U_t^2 in Fig. 8, and U_t^3 in Fig. 9, for the binary pulse X_t in Fig. 7. Here $(\sigma_v)^2 = 4$

the concealed data are for PGM in some way, and he/she has to write the header by himself/herself to restore the pictorial image.

As for the role of the common key $v^i(t)$, comparing Fig. 12 with Fig. 11, we can realize the effect of the variance of the common key $v^i(t)$ and the nonlinear function

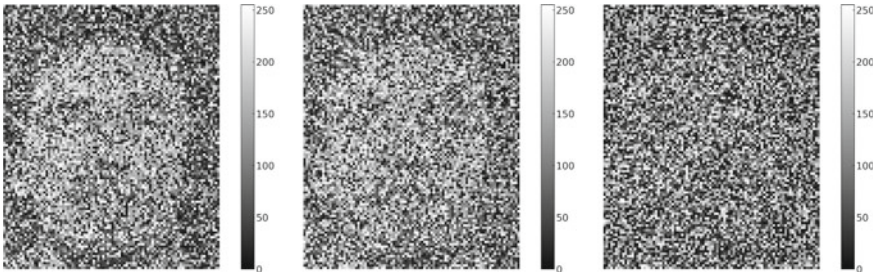

Fig. 12 From the left, pictorial images of the concealed data, U_t^1, U_t^2 in Fig. 8, and U_t^3 in Fig. 9, for the binary pulse X_t in Fig. 7. Here $(\sigma_v)^2 = 1$

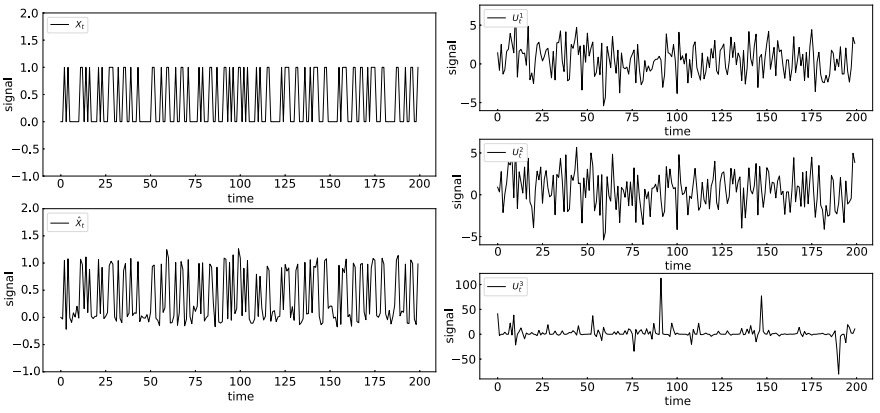

Fig. 13 X_t (Fig. 7) and $\widehat{X}_t$ (Fig. 10) from the above of the left 2 graphs. U_t^1 (Fig. 8), U_t^2 (Fig. 8), and U_t^3 (Fig. 9) from the above of the right 3 graphs. Here $t \in [0, 200]$ only

$f(\xi)$. The variance of the common key $v^i(t)$ is smaller in Fig. 12 than it is in Fig. 11, that is, $(\sigma_v)^2 = 4$ for Fig. 11 and $(\sigma_v)^2 = 1$ for Fig. 12, though other parameters for Fig. 12 are the same as for Fig. 11. The contour of the face in the pictorial image of U_t^1 in Fig. 12 stands out more clearly than in Fig. 11. Meanwhile, the nonlinearity conceals the contour as in the pictorial image of U_t^3 in Fig. 12.

In Fig. 13 we show the comparison of the original binary pulse X_t, its restoration $\widehat{X}_t$, and the concealed data U_t^i, $i = 1, 2, 3$.

4.2 Analog Data of Pictorial Image

We use analog data of a pictorial image in the Olivetti faces database (The Olivetti Faces Database 2020), where the data of pictorial images are transformed to analog data from the original ones in the ORL Database of Faces, an archive of AT&T

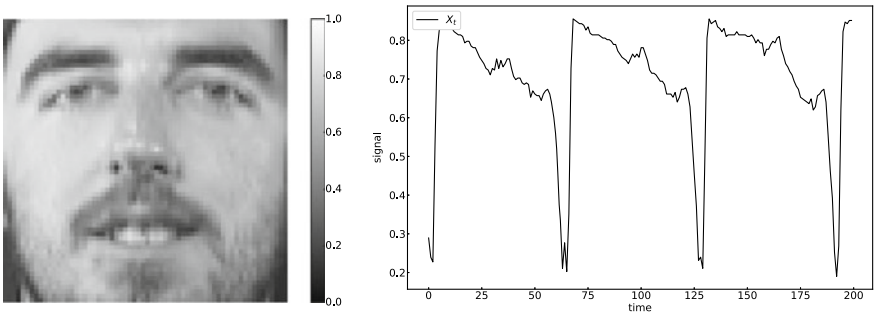

Fig. 14 The original pictorial image (left) with the analog data, and the analog data X_t only for $t \in [0, 200]$ (right)

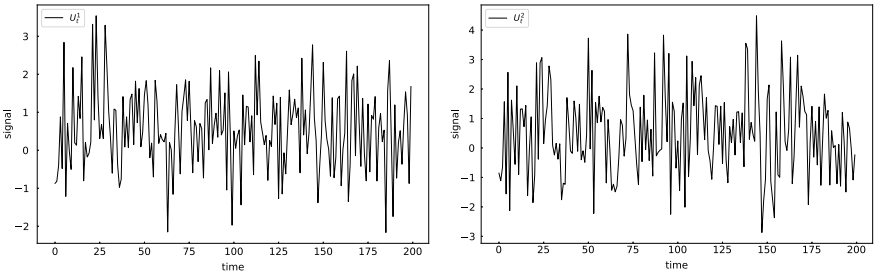

Fig. 15 The concealed data, U_t^1 (left) and U_t^2 (right), for the analog data X_t in Fig. 14. Here, $t \in [0, 200]$ only

Laboratories Cambridge (The ORL Database of Faces 2020). The data have the grayscale value of 256 gradations (8bit/pixel). Our parameters are $A = A^i = 0.1$, $b = b^i = 1$, $b_u = b_u^i = 1$, $c = c^i = 1$, $\sigma_1 = \sigma_1^i = 0.1$, and $\sigma_2 = \sigma_2^i = 1$ again. We also use the common key $v^i(t)$ in the same way as in Sect. 3.2 with $\sigma_v = 2$. The original analog data X_t and their pictorial image are in Fig. 14. Here, the upper bound of t is $64 \times 64 = 4096$ and t runs over $[0, 4096]$. The concealed data, U_t^1 and U_t^2, defined by Eq. (7) are in Fig. 15, and the concealed data U_t^3 defined by Eq. (3) are in Fig. 16. We can restore the pictorial image with the restoration $\widehat{X}_t$ as in Fig. 17. If a wiretapper becomes aware of our method to make a pictorial image from analog data, then the wiretapper gets pictorial images from the concealed data U_t^i, $i = 1, 2, 3$, as in Fig. 18.

In Fig. 19 we show the comparison of the original binary pulse X_t, its restoration $\widehat{X}_t$, and the concealed data U_t^i, $i = 1, 2, 3$.

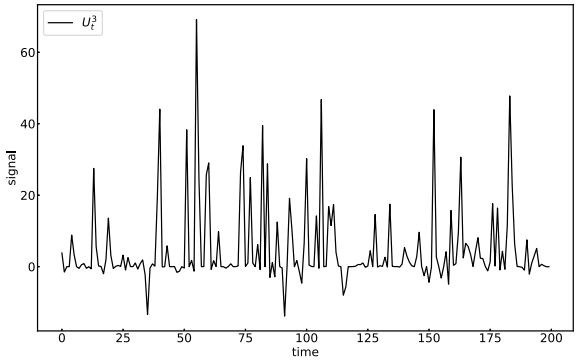

Fig. 16 The concealed data U_t^3 for the analog data X_t, $t \in [0, 200] \subset [0, 4096]$, in Fig. 14

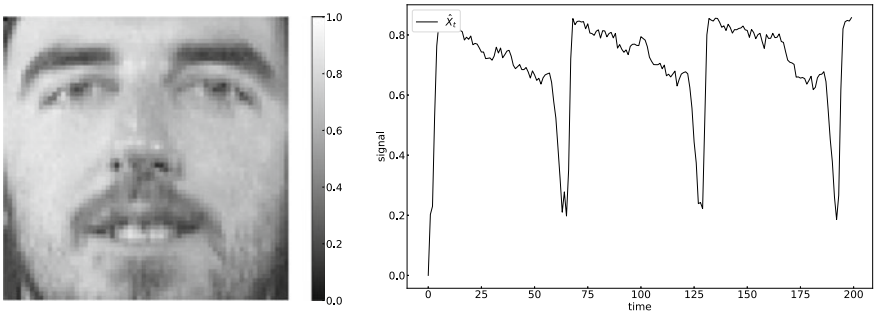

Fig. 17 The restoration $\widehat{X}_t$ (right) for the analog data X_t in Fig. 14 only for $t \in [0, 200]$, and the pictorial image (left) of $\widehat{X}_t$

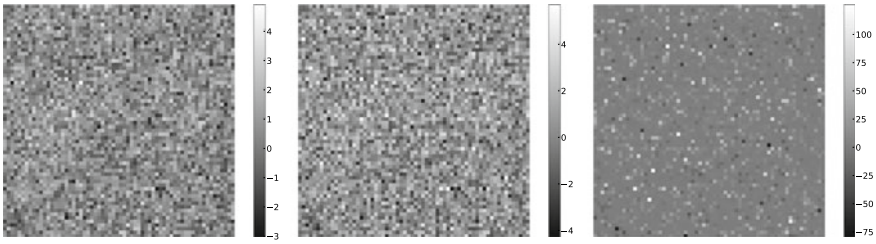

Fig. 18 From the left, pictorial images of the concealed data, U_t^1 (Fig. 15), U_t^2 (Fig. 15), and U_t^3 (Fig. 16)

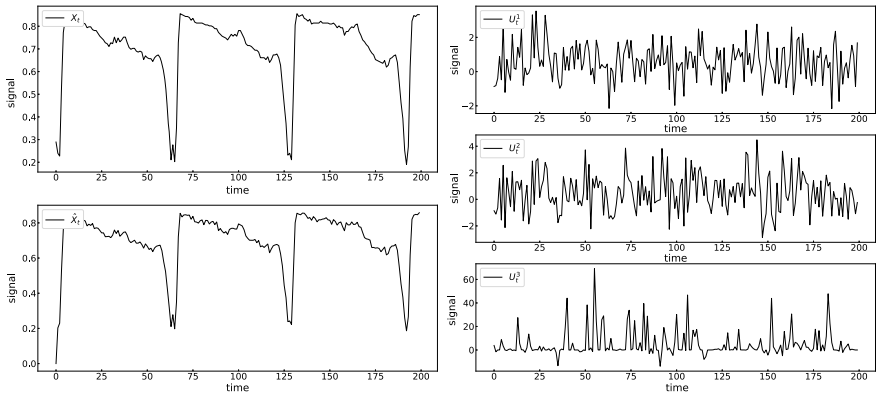

Fig. 19 X_t (Fig. 14) and $\widehat{X}_t$ (Fig. 17) from the above of the left 2 graphs. U_t^1 (Fig. 15), U_t^2 (Fig. 15), and U_t^3 (Fig. 16) from the above of the right 3 graphs. Here $t \in [0, 200]$ only

5 Conclusion and Future Work

We have proposed a mathematical technique for concealing data on the physical layer of the OSI reference model by using random noise disturbance, and moreover, a mathematical technique for restoring the concealed data by using the stochastic process estimation. In this concealing-restoring system, the functionals determining SDEs play a role of secret or common keys. Then, the proper noise-filtering theory forms a nucleus to restore the concealed data. In addition, we have showed the simulation result for the data on physical layer and some applications of the two techniques to the pictorial images. We have opened one of examples of the functionals. Then, we have showed how to conceal the data by using the noise-disturbance, and have demonstrated how to restore the data by removing the noises. Here, the significant point to be emphasized is that any composition of the SES and any form of the individual functional will do so long as a proper noise-filtering method is established for them. We make briefly some comments about it at the tail end of this section.

We have used the scalar-valued processes, and thus, prepared just one common key for one SDE. We can prepare some common keys for one SDE by using the vector-valued processes.

Although we have employed the message digest to make the check of the coincidence of the binary word and the detection of the falsification at the same time, we are now developing a method with low complexity so that we can make them for data on the physical layer.

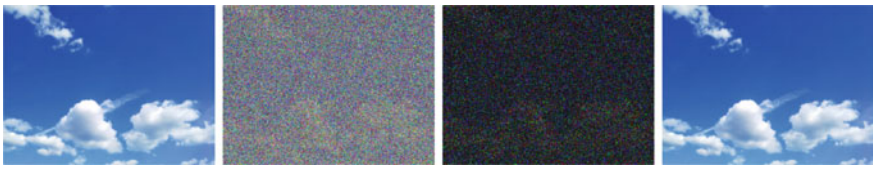

Fig. 20 From the left, the original pictorial image, the individual pictorial images of the concealed data U_t^1 and U_t^2, and the pictorial image of the restored data. The original pictorial image is a bitmap image, and the parameter t of the original data X_t runs over [0, 90123byte]

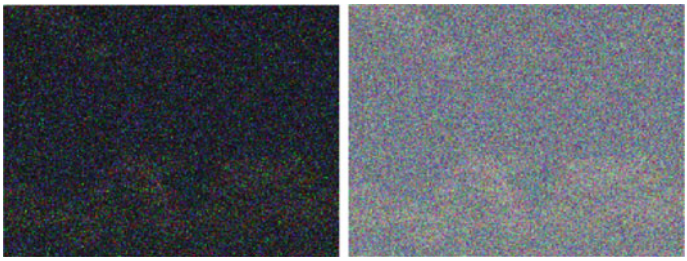

Fig. 21 Comparison between the pictorial images of U_t^2 with nonlinearity (left) and $X_t^2 = f^{-1}(U_t^2)$ without nonlinearity (right)

According to our several experiments including the concrete examples in Sect. 4, we think that the nonlinearity enhances the noise-disturbance. For instance, the pictorial images in Fig. 20 are the case $N = 1$. Comparing the pictorial images of U_t^2 and $X_t^2 = f^{-1}(U_t^2)$ in Fig. 21, we can say that the enhancement of noise-disturbance appears with the black color. We will study the roles of several parameters including the nonlinearity. We here introduce the effect coming from the nonlinearity beforehand. The state space determined by Eq. (5) is constructed by the linear Gaussian model, and thus, we used the linear Kalman filtering theory in Sects. 3 and 4. We can make it more general: nonlinear, non-Gaussian state space. Then, we should employ another noise-filtering theory such as the particle filtering theory (Bain and Crisan 2009). In fact, putting a concrete nonlinearity N_A or another nonlinearity N_B in the functional F_i of Eq. (1), we have concealed data $U_t^{A,i}$ or $U_t^{B,i}$, $i = 1, 2, 3$, different from those in this paper. Then, the linear Kalman filtering theory is not useful any longer. For instance, we respectively conceal the data in Figs. 7 and 14 using such functionals with the nonlinearity N_A or N_B. Then, we cannot estimate the data from the concealed ones by the linear Kalman filter to our satisfaction. See Figs. 22, 23, 24, and 25. The difference between the restorations in Figs. 22 and 23 or between those in Figs. 24 and 25 depends on the degree of nonlinearity. We show the restoring system using the particle filter in Ref. Fujii and Hirokawa (2020).

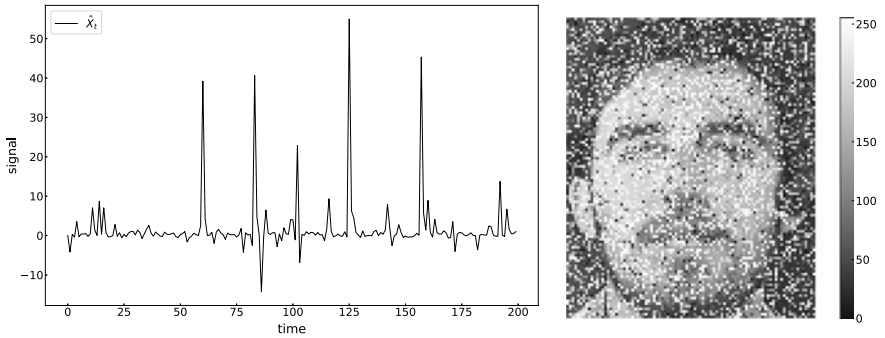

Fig. 22 The left graph is restoration $\widehat{X}_t$, $0 \leq t \leq 200$, from the concealed data, $U_t^{A,i}$, $i = 1, 2, 3$, with the nonlinearity N_A using the Kalman filtering. The right picture is the pictorial image restored from such a restoration $\widehat{X}_t$

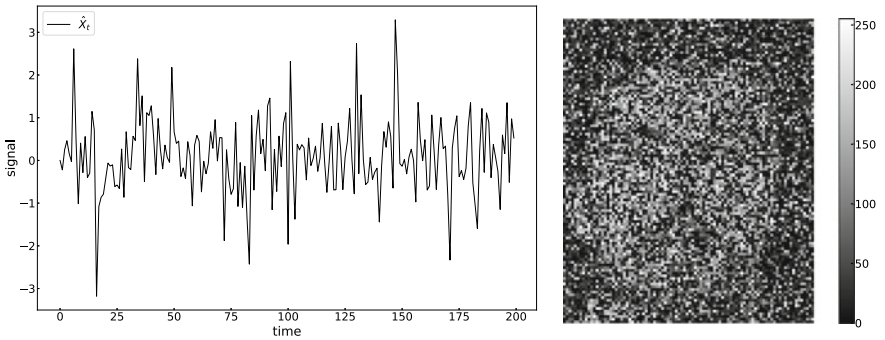

Fig. 23 The left graph is restoration $\widehat{X}_t$, $0 \leq t \leq 200$, from the concealed data, $U_t^{B,i}$, $i = 1, 2, 3$, with the nonlinearity N_B using the linear Kalman filtering. The right picture is the pictorial image restored from such a restoration $\widehat{X}_t$

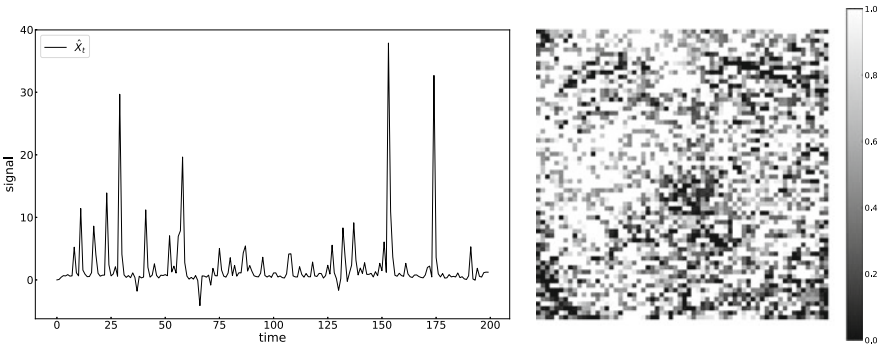

Fig. 24 The left graph is restoration $\widehat{X}_t$, $0 \leq t \leq 200$, from the concealed data, $U_t^{A,i}$, $i = 1, 2, 3$, with the nonlinearity N_A using the linear Kalman filtering. The right picture is the pictorial image restored from such a restoration $\widehat{X}_t$

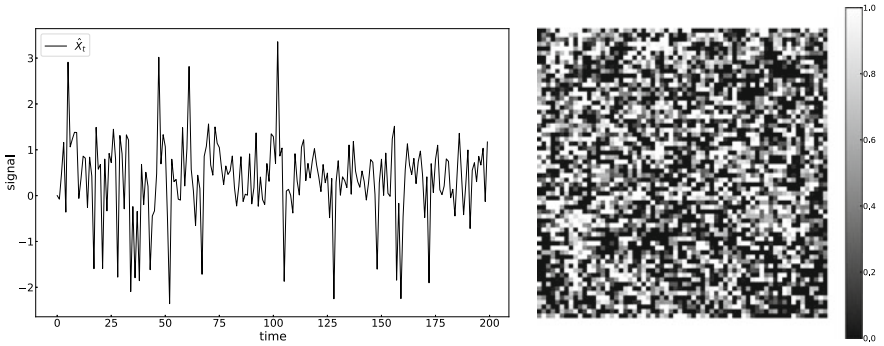

Fig. 25 The left graph is restoration $\widehat{X}_t$, $0 \leq t \leq 200$, from the concealed data, $U_t^{B,i}$, $i = 1, 2, 3$, with the nonlinearity N_B using the Kalman filtering. The right picture is the pictorial image restored from such a restoration $\widehat{X}_t$

Acknowledgements This work is partially based on Fujii's bachelor thesis at Hiroshima University in March, 2019. For useful comments and discussion, the authors thank the following: Kirill Morozov (University of North Texas), Shuichi Ohno (Hiroshima University), Kouichi Sakurai (Kyushu University), Takeshi Takagi (Hiroshima University), and Tatsuya Tomaru (Hitachi, Ltd.).

References

A. Bain, D. Crisan, *Fundamentals of Stochastic Filtering* (Springer, Berlin, 2009)
J. Clausen, E. Fetz, J. Donoghue, J. Ushiba, U. Spörhase, J. Chandler, N. Birbaumer, S.R. Soekadar, Help, hope, and hype: ethical dimensions of neuroprosthetics. Science **356**, 1338–1339 (2017)
K.M. Cuomo, A.V. Oppenheim, Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Trans. Circuit Syst. **40**, 626–633 (1993)
I. Damgård, A design principle for hash functions, in *Advances in Cryptology – CRYPTO'89 Proceedings*. Lecture Notes in Computer Science, vol. 435 (Springer, 1989), pp. 416–427
T. Fujii, M. Hirokawa, Nonlinear concealing-restoring system with random noise disturbance for data on physical layer arXiv:1910.03214
S. Goel, R. Negi, Guaranteeing secrecy using artificial noise. IEEE Trans. Wirel. Commun. **7**, 2180–2189 (2008)
G. Grassi, S. Mascolo, A system theory approach for designing cryptosystems based on hyperchaos. IEEE Trans. Circuit Syst. -I: Fundam. Theory Appl. **46**, 1135–1138 (1999)
M.S. Grewal, A.P. Andrews, *Kalman Filtering. Theory and Practice Using MATLAB* (Wiley, New York, 2015)
A. Hero, Secure space-time communication. IEEE Trans. Inf. Theory **49**, 3235–3249 (2003)
K. Ito, Y. Masuda, E. Okamoto, A chaos MIMO-based polar concatenation code for secure channel coding, in *2019 International Conference on Information Networking* (2019), pp. 262–267
B.N. Kain, A.K. Agrawala, *Open Systems Interconnection: Its Architecture and Protocols* (McGraw-Hill, London, 1992)
G. Kallianpur, *Stochastic Filtering Theory* (Springer, Berlin, 1980)
R.E. Kalman, A new approach to linear filtering and prediction problems. Trans. ASME - J. Basic Eng. (Ser. D) **82**, 35–45 (1960)

H. Lenug, J. Lam, Design of demodulator for the chaotic modulation communication system. Trans. Circuit Syst. **44**, 262–267 (1997)
C. Lin, D. He, N. Kumar, K.-K.R. Choo, A. Vinel, X. Huang, Security and privacy for the internet of drones: challenges and solutions. IEEE Commun. Mag. **56**, 64–69 (2018)
R.C. Merkle, Secrecy, authentication, and public key systems, Ph.D. thesis (Stanford University, 1979)
R.C. Merkle, A certified digital signature, in *Advances in Cryptology - CRYPTO'89 Proceedings*. Lecture Notes in Computer Science, vol. 435 (Springer, 1989), pp. 218–238
MessageDigest, Android developers, https://developer.android.com/reference/java/security/MessageDigest
A. Mukherjee, A.L. Swindlehurst, Robust beam-forming for security in MIMO wiretap channels with imperfect CSI. IEEE Trans. Signal Process. **59**, 351–361 (2011)
S. Ohno, H. Kaida, T. Kodani, Secret communication with multiple antennas may not be secure against eavesdropping using blind equalization (in Japanese). IEICE Trans. Commun. **J95-B**, 751–759 (2012)
E. Okamoto, A chaos MIMO transmission scheme for secure communications on physical layer, in *Proceedings of the 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)* (2011), pp. 1–5
E. Okamoto, Y. Inaba, A chaos MIMO transmission scheme using turbo principle for secure channel-coded transmission. IEICE Trans. Commun. **E98.B**, 1482–1491 (2015)
E. Okamoto, Y. Iwanami, A trellis-coded chaotic modulation scheme, in *2006 IEEE International Conference on Communications*, vol. 11 (2006), pp. 5010–5015
R. Rivest, The MD4 message digest algorithm, in *Advances in Cryptology - CRYPTO'90 Proceedings*. Lecture Notes in Computer Science, vol. 37 (Springer, 1991), pp. 303–311
R. Rivest, The MD4 message digest algorithm. RFC **1320** (1992a) (MIT and RSA Data Security, Inc.)
R. Rivest, The MD5 message digest algorithm. RFC **1321** (1992b) (MIT and RSA Data Security, Inc.)
R. Román-Castro, J. López, S. Gritzalis, Evolution and trends in IoT security. Computer **51**, 16–25 (2018)
B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C* (Wiley, New York, 2015)
Secure hash standard (SHS), FIPS PUB 180-4, Federal Information Processing Standards Publication (2015)
S.b. Suhaili, T. Watanabe, High-throughput message digest (MD5) design and simulation-based power estimation using unfolding transformation. J. Signal Process. **21**, 233–238 (2017)
A.L. Swindlehurst, Fixed SINR solution for the MIMO wiretap channel, in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing* (2009), pp. 2437–2440
The Olivetti faces database, https://scikit-learn.org/0.19/datasets/olivetti_faces.html
The ORL database of faces, https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html
C.W. Wu, L.O. Chua, A simple way to synchronize chaotic systems with applications to secure communication systems. Int. J. Bifurc. Chaos **3**, 1619–1627 (1993)
A.D. Wyner, The wire tap channel. Bell Syst. Tech. J. **54**, 1355–1387 (1975)
H.Y. Youm, An overview of security and privacy issues for internet of things. IEICE Trans. Inf. Syst. **E100–D**, 1649–1662 (2017)
G. Zheng, Secure communication based on multi-input multi-output chaotic system with large message amplitude. Chaos Solitons Fractals **41**, 1510–1517 (2009)