Recommended Paper

Effects of Data Hiding on Remote Data Analysis

Kanta Matsuura†

When digital data are distributed over an open network, they do not always keep their original bit-strings: for example, issues related to copyright protection may necessitate the use of digitally watermarked images. When we want to use a watermarking system, there is a requirement that the data be kept *acceptable*. Usually, the difference between the original data and the watermarked data is evaluated by human recognition; for instance, if users cannot notice the difference visually, the watermark is considered acceptable. We here suggest another scenario: if the user is not a human being but a remote computer which analyzes the digital data, the acceptance criteria might be different. This paper studies how data hiding affects remote data analysis. Specifically, a design competition among remote computers is simulated. The result suggests the importance of how the design problem is represented; smaller condition numbers of the coefficient matrix provide better robustness of the competition when the signal-to-noise ratio (SNR) is sufficiently high. This effect is demonstrated by means of a phantom-experiment study.

1. Introduction

Once equipped with security mechanisms, open networks can be used for a wider range of applications. Let us imagine an application in which digital data distributed over a network do not keep their original bit-strings completely unchanged, as in the case of digitally watermarked images[1)~4)]. In this example, the difference between the original images and the watermarked images is usually evaluated by human recognition; if the user does not notice the difference by looking at the images, the watermarking is considered acceptable, that is, the images are regarded as being as good as the original ones.

In different applications where not a human user but a computer itself uses the digital data, however, the evaluation criteria might be different. For instance, we may watermark our own measured data and then entrust the analysis of the data to a remotely located third-party computer (see **Fig. 1**). What if the watermarked data give us results quite different from those given by the original data? We may also watermark our own design criteria and then entrust the specific design to a third party. What if the watermarked criteria give us a solution that is too different from the solution given by the original criteria? In accordance with the application, we should use an appropriate strategy to evaluate the effects of watermarking or data hiding.

This paper studies the effects of data hiding on remote data analysis. The basic procedures are introduced in Section 2. Section 3 then describes a simulation using these procedures. In Section 4, after discussing the implication of the

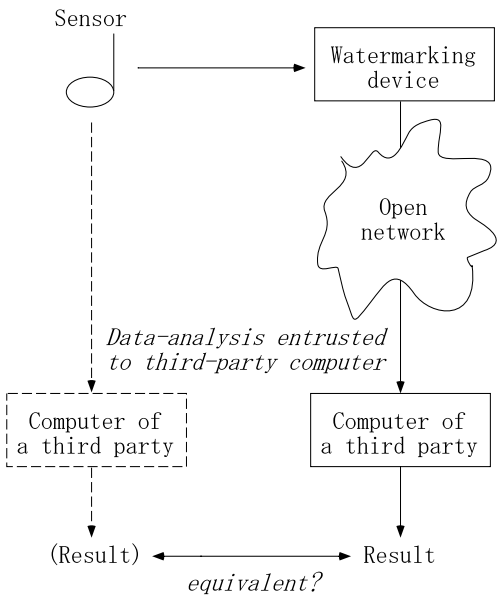


Fig. 1 Entrusting the analysis of remotely measured and then watermarked data to third-party computers.

† Institute of Industrial Science, the University of Tokyo

The initial version of this paper was presented at the CSS'99 workshop held on Oct. 1999, which was sponsored by CSEC. This paper was recommended to be submitted to the Journal of IPSJ by the chairperson of CSEC.

simulation results, we demonstrate what happens in an actual measurement and its analysis. Finally, Section 5 offers some concluding remarks.

2. Basic Procedures

2.1 Random Data Hiding

Let $\boldsymbol{y} = (y_1, y_2, \cdots, y_N)^T$ be a set of measurements or design criteria☆. Without referring to a specific data-hiding algorithm, we consider the following procedures:

(1) Randomly choose a specified number of measurements $(y_{j_1}, y_{j_2}, \cdots, y_{j_n})^T$.

(2) The chosen measurements are disturbed by white noise.

In the following, n/N is referred to as the *density* of this data hiding. Denoting the disturbed data by $\tilde{\boldsymbol{y}}$, we define the signal-to-noise ratio (SNR) as

$$SNR = 20 \log \frac{||\boldsymbol{y}||}{||\tilde{\boldsymbol{y}} - \boldsymbol{y}||}. \tag{1}$$

2.2 Generalized Inversion

Let us consider a system equation

$$A\boldsymbol{x} = \boldsymbol{y}, \tag{2}$$

where $A = (a_{i,j})$ is a system *coefficient matrix* and $\boldsymbol{y}$ is a given measurement. $\boldsymbol{x} = (x_1, x_2, \cdots, x_M)^T$ is a set of *design parameters* to be used by a third-party computer. For simplicity, we assume that A is full-ranked.

When the dimension of $\boldsymbol{x}$ is smaller than that of $\boldsymbol{y}$ (i.e., $M < N$), the system equation (2) cannot be completely satisfied. In other words, the system is overdetermined. In this overdetermined case, a generalized-inverse (or pseudoinverse) matrix

$$A^+ \equiv \left(A^T A\right)^{-1} A^T \tag{3}$$

of A is used to obtain a minimum square-error estimate

$$\boldsymbol{x}^+ = A^+ \boldsymbol{y}, \tag{4}$$

where $\boldsymbol{x}^+$ is the solution of a minimum square-error problem

$$||A\boldsymbol{x} - \boldsymbol{y}|| \to \min. \tag{5}$$

When $M = N$, the system equation (2) has a unique solution $\boldsymbol{x}{=}A^{-1}\boldsymbol{y}$. In other words, the system is well determined. Depending on the design constraint, however, the third party may encounter an overdetermined problem even if $M = N$; if the client wants to reduce the number of parts, the number of non-zero parameters may be limited☆☆. Let us suppose that only m ($< M$) parameters are allowed to be non-zero. In this case, the third party would search for the set of values $(i_1, i_2, \cdots, i_m)$ that minimizes the error

$$\left|\left| A_{(i_1,i_2,\cdots,i_m)} \begin{pmatrix} x_{i_1} \\ x_{i_2} \\ \vdots \\ x_{i_m} \end{pmatrix} - \boldsymbol{y} \right|\right| \tag{6}$$

where the coefficient matrix in Eq. (6) is given by

$$A_{(i_1,i_2,\cdots,i_m)} = \begin{pmatrix} a_{1,i_1} & a_{1,i_2} & \cdots & a_{1,i_m} \\ a_{2,i_1} & a_{2,i_2} & \cdots & a_{2,i_m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N,i_1} & a_{N,i_2} & \cdots & a_{N,i_m} \end{pmatrix}. \tag{7}$$

An exhaustive search could be described as follows:

(1) Choose $(i_1, i_2, \cdots, i_m)$ and set the error $E = \infty$.

(2) Compute a minimum-square error solution for $(i_1, i_2, \cdots, i_m)$ as $\boldsymbol{x}^+_{(i_1,i_2,\cdots,i_m)} = (0,\ 0,\ \cdots,\ 0,\ x_{i_1},\ 0,\ \cdots,\ 0,\ x_{i_2},\ 0,\ \cdots,\ 0,\ x_{i_m},\ 0,\ \cdots,\ 0)^T$, where $(x_{i_1},\ x_{i_2},\ \cdots,\ x_{i_m})^T = A^+_{(i_1,i_2,\cdots,i_m)}\boldsymbol{y}$.

(3) If $\left|\left| A\boldsymbol{x}^+_{(i_1,i_2,\cdots,i_m)} - \boldsymbol{y} \right|\right| < E$, then take $\boldsymbol{x}^+_{(i_1,i_2,\cdots,i_m)}$ as a temporary solution and set $E = \left|\left| A\boldsymbol{x}^+_{(i_1,i_2,\cdots,i_m)} - \boldsymbol{y} \right|\right|$.

(4) Change $(i_1, i_2, \cdots, i_m)$ and return to Step (2).

It should be noted that the problem above is not a simple parameter fitting. We must select m (out of M) parameters which take non-zero values so that the resultant square-error fitting problem gives the "minimum of the minimum errors" among all the possible selections; for each selection (Step (1) or (4)), we solve the square-error problem (Step (2)), and search for the optimum selection (Step (3)). What the selection really means depends on the application. An example is given later in Section 4.2.

3. Effects of Data Hiding

3.1 Situation

In order to avoid disturbance by computational round-off error, a small-scale situation $M = N = 10$ is considered. The coefficient matrix A and the measurement vector $\boldsymbol{y}$ are randomly generated. $\boldsymbol{y}$ is then watermarked to

☆ Transpose is represented by ^{T}.

☆☆ In the design of beamforming arrays, for example, the number of arrays is reduced as the solution becomes more sparse[5].

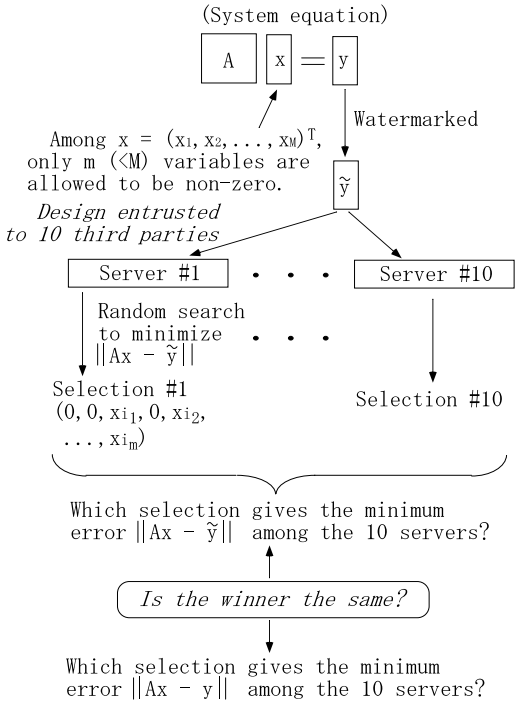


Fig. 2 Design competition among remote servers. If the winner is the same with and without the watermark, the watermark is evaluated as acceptable in the sense that the competition is robust enough. We repeat the illustrated procedure and see how often the watermark is accepted.

be $\tilde{\boldsymbol{y}}$ with a density of 0.4. A client entrusts the design to 10 third parties. These parties are called *servers* in the following discussion. The servers are allowed to select at most $m = 3$ nonzero design parameters and search for a better selection by the random search procedure described in the previous section. Each random search is iterated 10 times.

3.2 Evaluation Criterion

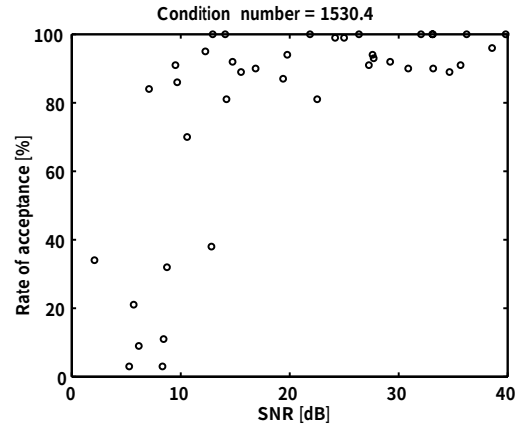
Among the results from all the servers, the client finds the best one in terms of the square error. The server which gives this minimum error is called the *winner*. By definition, the winner is the best in terms of the error for the watermarked data $\tilde{\boldsymbol{y}}$. However, it is not guaranteed that the winner's selection gives the minimum error for the original data $\boldsymbol{y}$ as well. If this is guaranteed, we can use the watermarking without affecting the competition.

Unfortunately, we cannot have such a guarantee in general. This in turn motivated us to define an evaluation criterion as follows:

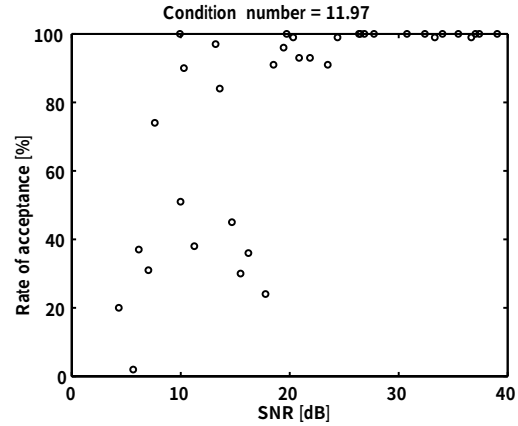
(1) For the final parameter selection by each server, the error not for the watermarked data $\tilde{\boldsymbol{y}}$ but for the original data $\boldsymbol{y}$ is computed.

(2) If the winner is still best in terms of this error, the data-hiding is regarded as *acceptable* in terms of robustness.

This procedure is summarized in **Fig. 2**. After repeating the procedure, we saw how often the data hiding was accepted. This rate was defined as the *rate of acceptance* and used as an evaluation criterion.



(a) $cond(A) = 1530.4$



(b) $cond(A) = 11.97$

Fig. 3 Rate of acceptance vs. SNR. $cond(A)$ represents the condition number of the system coefficient matrix A.

3.3 Results

For each set of A and $\boldsymbol{y}$, the simulation is carried out $K = 100$ times. Let the number of acceptances (= the number of times the data hiding is accepted) be L. The rate of acceptance L/K is then given as in **Fig. 3**. The simulation was carried out by using two different system

matrices whose condition numbers[☆] were very different; one was 1530.4 while the other was 11.97. Since we consider random matrices of small size (10×10), we assume that the computation of condition numbers is precise enough for the discussion in the next section.

4. Discussion

4.1 Implication

We first discuss the implications of the simulation results.

In linear estimation theory, the condition number of a system coefficient matrix is in close relation to the robustness against errors[6]; larger condition numbers cause larger disturbances or larger error distributions.

The results in Fig. 3 suggests that

(I) for high SNRs, a smaller condition number is better

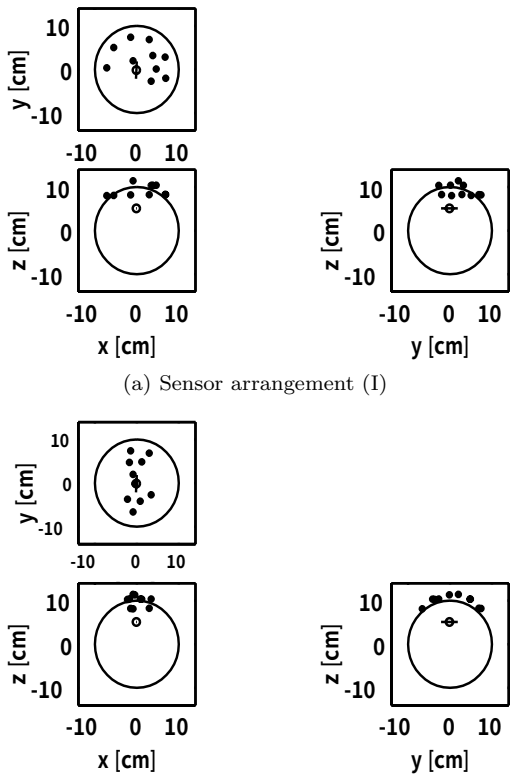
and that

(II) for low SNRs, a difference in condition number has insignificant effects.

In the simulated situation, a threshold SNR between (I) and (II) is estimated to be around 18 dB.

The condition number depends on how the design problem is represented. When data-hiding algorithms are efficient enough to yield SNRs much higher than the threshold, the particular representation of the problem is important for reliable analysis.

Medical-image processing can be a good application of data hiding because it introduces privacy issues. For example, in a biomagnetic imaging system, how to determine the active positions in a human brain or heart is a fundamental problem[7)~9)]. In the competition scenario considered in this paper, each component of the vector $\boldsymbol{y}$ represents the magnetic flux density measured by each magnetic sensor. Selection from the components of the vector $\boldsymbol{x}$ corresponds to the estimation of the active points in the human brain or heart. The system coefficient matrix A depends on the arrangement of the sensors, including the types of the detection coils used[☆☆]. Our simulation results suggest that the arrangement of the magnetic sensors could be optimized in terms of the robustness against data-hiding.



(a) Sensor arrangement (I)

(b) Sensor arrangement (II)

Fig. 4 Magnetic-sensor distribution around a spherical phantom with a radius of 10.0 cm. Each arrangement has 10 sensors. A dipole electrode is located at $(-0.11, -0.14, 5.10)$ [cm] and is directed as indicated by the small circle and line (ϕ).

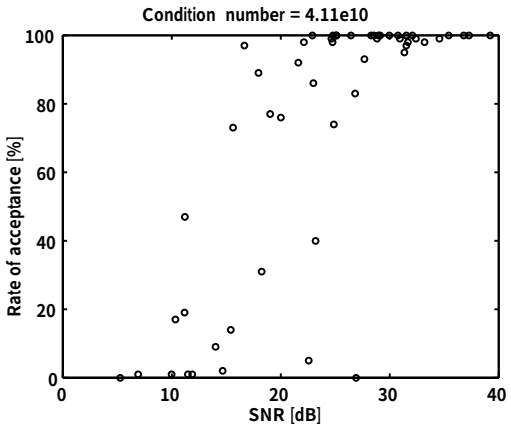
4.2 Demonstration by Phantom Data

Next, we demonstrate the effect of better condition numbers by using phantom-experiment data measured around a saline-filled spherical phantom with a radius of 10.0 cm. The phantom simulated a human brain and was set up in a magnetically shielded room. The phantom had a dipole electrode inside. The electrode simulated neural activity by a spiked current or a current dipole[☆☆☆]. The resultant magnetic signals (magnetic-flux density bandpassed between 0.1 and 100 Hz) were sequentially recorded at $N = 10$ locations. We used two different sensor arrangements, shown in **Fig. 4**. The electrode was located at

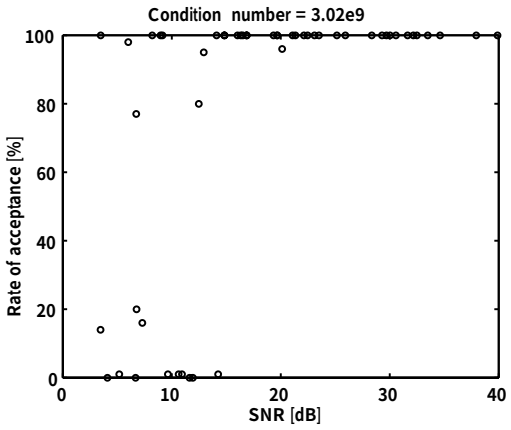
☆ The condition number of a matrix is defined as the ratio of the largest to the smallest singular values of the matrix. The actual value depends on the definition of the norm. This paper uses the most popular square norm in Euclidean space.

☆☆ For example, three-dimensional coils provide different coefficients[10)~12)].

☆☆☆ The dipole moment of a current dipole is defined as $I \cdot \delta x$ [A·m], where I is its electric current and δx is its length (typically very short).



(a) For sensor arrangement (I)



(b) For sensor arrangement (II)

Fig. 5 Rate of acceptance vs. SNR for different sensor arrangements. Sensor arrangement (II) gives the smaller condition number and better robustness.

$(-0.11, -0.14, 5.10)$ [cm] and the manual location error was estimated to be below 0.2 cm. The direction of the current dipole at the electrode was $(0.05, 0.99, 0.00)$. The two sensor arrangements give different condition numbers of the system coefficient matrix A; sensor arrangement (I) gives $cond(A) = 4.11 \times 10^{10}$, while sensor arrangement (II) gives $cond(A) = 3.02 \times 10^9$.

Equally-spaced $M = 10$ grid points $(0, 0, 0.5)$, $(0, 0, 1.5)$, $\cdots$, $(0, 0, 9.5)$ [cm] were set up along the z axis in the upper hemisphere ($z > 0$) of the phantom. The current-dipole moments (y-component) at these grid points were the design parameters to be determined. We allow two grid points to have non-zero moments and want to find the couple of points adjacent to the electrode: $(0, 0, 4.5)$ and $(0, 0, 5.5)$. This corresponds to a simplified version of a problem which asks us to find the active region along a given sulcus in the brain.

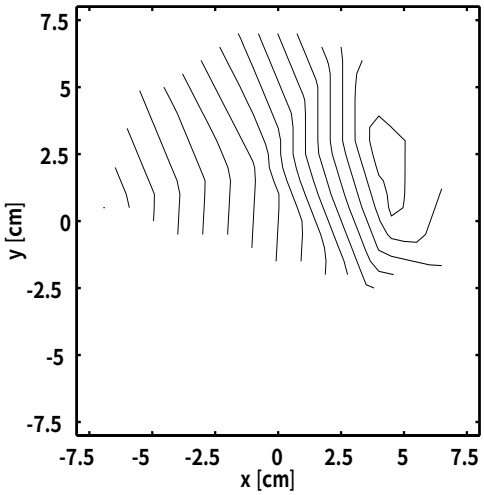


Fig. 6 Contour map of the original magnetic field measured by sensor arrangement (I).

The coefficient matrices for the two sensor arrangements were computed by using the Biot-Savart law. We then had a competition similar to that in Section 3:

- The measurement was watermarked with a density of 0.4 and sent to 10 servers.
- Each server replied after 10 iterations of the random search.
- By changing the watermark 100 times, we obtained the rate of acceptance defined in Section 3.3.

For different SNRs, we obtained the rates of acceptance shown in **Fig. 5**. Thus the sensor arrangement with the smaller condition number (*i.e.*, sensor arrangement (II)) gives better robustness, which is consistent with the result of the simulation.

4.3 Conventional Evaluation

Let us revisit the conventional idea of watermark evaluation[1)~4)]: in the case of watermarked images, if users do not notice the difference between the original image and the watermarked image by looking at them, the watermarking is regarded as acceptable. Examples in the previous subsection can show how this conventional evaluation does not work in the case of remote-data analysis by computers.

Figure 6 shows a contour map of the original magnetic flux density measured by sensor arrangement (I). If it is watermarked, it can be changed into **Fig. 7**. It can also be changed into **Fig. 8**. The former has an SNR of 23.3 dB.

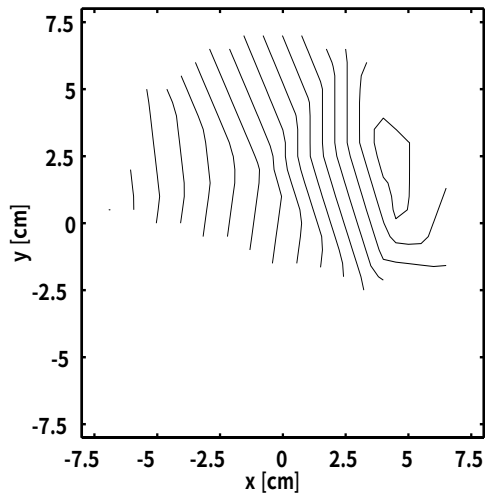


Fig. 7 Contour map of the watermarked magnetic field when the SNR is 23.3 dB.

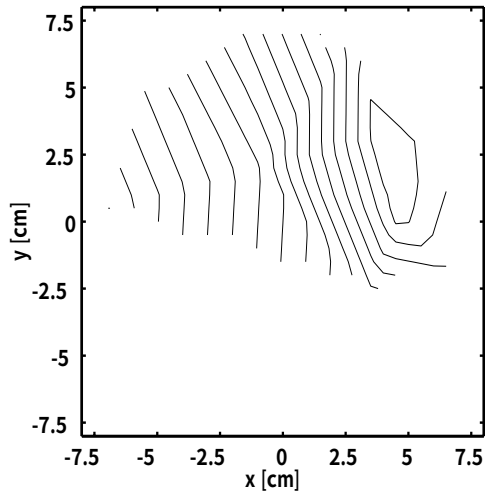


Fig. 8 Contour map of the watermarked magnetic field when the SNR is 35.8 dB.

Although this is lower than the threshold SNR found in Fig. 5 (a), conventional human recognition may accept the watermarked image as a good one. By contrast, the latter has an SNR of 35.8 dB. Although this is higher than the threshold SNR, human recognition may reject the watermarked image. Thus the criterion for remote-data analysis can be different from the conventional one.

5. Concluding Remarks

The effects of data-hiding were analyzed in the context of remote data analysis. Specifically, a design commitment competition was simulated. The result suggests the importance of the representation of a design problem; better-conditioned coefficient matrices contribute to more robust competition if the SNR is high enough. This finding was also supported by a hardware simulation using magnetic measurements around a spherical phantom.

The purpose of this paper is (1) to point out a new notion of acceptable data-hiding and (2) to outline the basic characteristics of such a notion by using a small problem which does not suffer from computational round-off errors. More quantitative analyses in the near future will include not only random setting of the problem but also particular examples such as medical image processing. This may contribute to an optimization of the sensor arrays as suggested by the demonstration.

Acknowledgments This work is supported by the 16th Research-Promotion Fund (No.28) from the Casio Science Promotion Foundation.

The author is very grateful to Dr. T. Imada and his colleagues at NTT Basic Research Laboratories for providing the phantom data.

References

1) Davis, J.C.: Protecting intellectual property in cyberspace, *IEEE Technology and Society Magazine*, Vol.17, No.2, pp.12–25 (1998).
2) Mano, T.: Information hiding into JPEG images, *Proc. 1999 Symposium on Cryptography and Information Security* (SCIS'99), Vol.II, pp.707–712 (1999).
3) Morimoto, N.: Digital watermarking technology (in Japanese), *J. IEICE*, Vol.82, No.8, pp.836–838 (1999).
4) Katzenbeisser, S. and Petitcolas, F. (Eds.): *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Publishers, London (2000).
5) Leahy, R.M. and Jeffs, B.D.: On the design of maximally sparse beamforming arrays, *IEEE Trans. Antennas Propagat.*, Vol.39, No.8, pp.1178–1187 (1991).
6) Healy, M.J.R.: *Matrices for Statistics*, Oxford University Press, New York (1986).
7) Tilg, B., Wach, P., Rucker, W. and Kynor, D.: Biomagnetic functional localisation: Iterative approach to estimation of electrical sources within the human heart from the magnetocardiogram, *Med. & Biol. Eng. & Comput.*, Vol.33, pp.238–240 (1995).
8) Matsuura, K. and Okabe, Y.: Selective minimum-norm solution of the biomagnetic inverse problem, *IEEE Trans. Biomed. Eng.*,

Vol.42, No.6, pp.608–615 (1995).
9) Matsuura, K. and Okabe, Y.: A robust reconstruction of sparse biomagnetic sources, *IEEE Trans. Biomed. Eng.*, Vol.44, No.8, pp.720–726 (1997).
10) Kobayashi, K. and Uchikawa, Y.: Estimation of multiple sources using a three-dimensional vector measurement of a magnetoencephalogram, *J. Appl. Phys.*, Vol.83, No.11, pp.6462–6464 (1998).
11) Kobayashi, K. and Uchikawa, Y.: Development of a three-dimensional biomagnetic measurement system with 39-channel SQUIDs, *Recent Advances in Biomagnetism*, Yoshimoto, T., Kotani, M., Kuriki, S., Karibe, H. and Nakasato, N. (Eds.), pp.35–38, Tohoku University Press, Sendai (1999).
12) Laine, P.P., Hämäläinen, M.S. and Ahonen, A.I.: Combination of magnetometers and planar gradiometers in an MEG system, *Recent Advances in Biomagnetism*, Yoshimoto, T., Kotani, M., Kuriki, S., Karibe, H. and Nakasato, N. (Eds.), pp.47–50, Tohoku University Press, Sendai (1999).

(Received February 14, 2000)
(Accepted June 19, 2001)

Editor's Recommendation

This paper deals with digital watermarking which is becoming to be very important topics in the field of illegal copy protection. The quality level of the research is high enough as recommendation paper.

(Chairman of CSEC Ryoichi Sasaki)

Kanta Matsuura was born in Osaka, Japan, in 1969. He received his B.E. degree in electrical engineering in 1992, an M.E. degree in electronics in 1994, and a Ph.D. degree in electronics in 1997, all from the University of Tokyo, Japan. He is currently a lecturer at the Institute of Industrial Science, University of Tokyo. His research interests include network and system security, optimization techniques, electronic commerce, and Internet technologies. He is a member of the IPSJ, the IEICE, and the IEEE.