Virtual Private Laboratories: Concept and Two Building Blocks[♦]

K. Matsuura
Interfaculty Initiative in Information Studies, University of Tokyo
Komaba 4-6-1, Meguro-ku
Tokyo 153-8505, JAPAN

***Abstract*-We are facing globalization of R&D activities over network involving different branches, companies, and organizations. These activities can be helped a lot by Internet. However, we have to be careful about security problems associated with such activities. The purpose of this paper is to identify the security problems and introduce the total system as a new concept: Virtual Private Laboratories (VPLs).**

Some of the identified problems are trivial but others are not; the former can be solved by a direct use of existing cryptographic primitives and protocols, whereas the latter needs new technologies and theories. Although all of them are necessary for VPLs, this paper is focused on two non-trivial building blocks and a theory: (1) academic database with multiple security functions, (2) data hiding for the purpose of entrusted data analysis, and (3) risk-management theory for digital objects secured by applied cryptography. In particular, (2) is studied in detail and difference from conventional data-hiding is shown with respect to evaluation criteria.

I. INTRODUCTION

We are facing globalization of R&D activities over network involving different branches, companies, and organizations. We know a lot of domestic examples (*e.g.* nano-technology consortium in Germany), and this trend is going to be international. These activities can be helped a lot by cheap and flexible use of Internet. However, since Internet is an open network, we have to be very careful about information-security problems [1]: access control, entity authentication, data secrecy, management of intellectual-property rights [2], availability [3, 4], and so on. The purpose of this paper is to identify the security problems and introduce a new concept for research-promotion infrastructure in the network era.

In particular, firstly the problems are described in Section II, which then introduces the total system as a new concept of *Virtual Private Laboratories (VPLs).* Among the problems, data hiding for VPLs is studied in detail in Section III. Finally Section IV concludes the paper.

II. VIRTUAL PRIVATE LABORATORIES

A. Open Network, R&D, and Security

Once equipped with security mechanisms, open networks can be used for wider range of applications. A good example is an electronic commerce [5]. We can develop on-line shopping protocols by using SSL/TLS [6]. We can construct digital payment or digital cash systems [7, 8] with the help of applied cryptography. Another emerging example is an e-government including electronic voting systems [9]. Thus, in an open network, we can find a lot of applications of information-security technologies for either commercial or administrative purposes.

Here we point out another possibility of making use of security technologies. Suppose a joint research project which involves researchers distributed over different companies/universities. The researchers exchange ideas with one another via e-mail. They download or browse digital publications as well as confidential tentative documents (*e.g.* design prototypes). They may have a video conference. They may complete on-line accounting forms. They want to share their ideas, bibliographic knowledge, information from their experiences (*e.g.* attendance at a conference), and so on. We can see that *a lot of security problems would appear in those academic/research activities over network.*

B. Security Problems

It is easy to make a list of trivial security issues. Suppose that all the researchers can use the same VPN (Virtual Private Network) [10] based on IPsec (IP security protocols) [11]. In the RFC on Security Architecture for the Internet Protocol [12], the set of security services that IPsec can provide includes *access control*, *connectionless integrity*, *data origin authentication*, *rejection of replayed packets*, *confidentiality*, and *limited traffic flow confidentiality*. In particular, the IP Authentication Header (AH) [13] provides connectionless integrity, data origin authentication, and an optional anti-replay service. The Encapsulating Security Payload (ESP) protocol [14] may provide confidentiality, and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service. Both AH and ESP can be vehicles for access control.

We then proceed to three non-trivial issues: two building blocks and one basic but new theory.

The first one is an architecture of a secure database designed for the networked academic/research activities. Suppose that we want to protect a data set composed of multiple attributes/components, and that each of them needs its own security property. One text component may have to be encrypted. Another text component may have to be encrypted as well as digitally signed. An image component may have to be watermarked. Another component may contain only the message authentication code (MAC) of a specific region of the data. Some of them may have to be associated with a secure audit log [15]. These requirements may lead us to *Provision-Based Access Control (PBAC)* [16] in which an access request is authorized *provided the requester takes certain security actions*. For example, we may have a

[♦] This work is partly supported by a research fund from International Communications Foundation.

situation where an entity X is allowed to have a write-access to data component Y *on condition that* X encrypts Y with a specific key K_1 and generates a specific entry to a secure audit log. However, the use of PBAC for networked research is not trivial, and due to the space limitation, unfortunately details are beyond the scope of this paper.

The second is related with protection of intellectual-property rights. Suppose that digital data distributed over the network do not exactly keep their original bit-strings due to the use of watermarking. When we use watermarking for the purpose of copyright protection of digital images [17], the difference between the original 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 acceptable. This is a conventional scenario. On the other hand, in the case of research promotion infrastructure, *not a human user but a computer itself uses the digital data*, and thus 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 (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 ask the specific design to a third party. What if the watermarked criteria give us a too different solution? In accordance with the application, we should use an appropriate strategy to evaluate the effects of watermarking or data-hiding. We will revisit this in detail later in Section III.

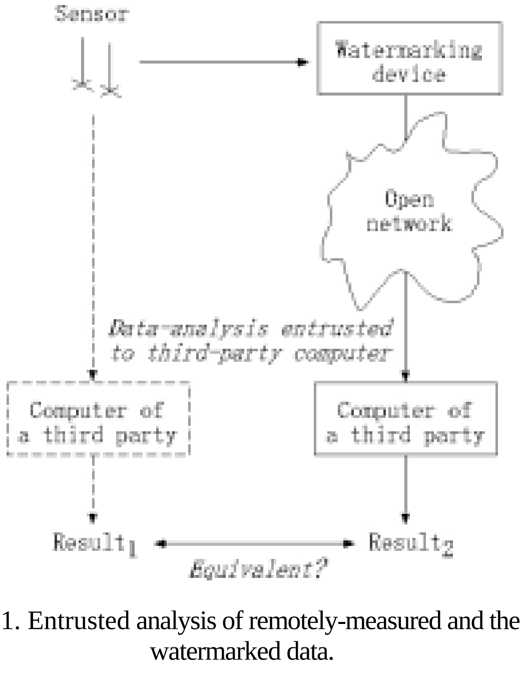

Sensor
Watermarking device
Open network
Data-analysis entrusted to third-party computer
Computer of a third party
Computer of a third party
Result1
Result2
Equivalent?

Fig. 1. Entrusted analysis of remotely-measured and then watermarked data.

Finally, the third issue is the risk management theory in the networked research cooperation where financial transactions are involved. In short, *the risk is from an unpredictable change of security/trust-related parameters over time*. This is, at a first glance, hard to believe; since digital objects can keep their original bit strings virtually forever, one may expect that there would be no risk of change. This is, unfortunately, not always the case. Digital objects can have not only prices but also other important stochastic values. For example, digital certificates may have confidence values or trust metrics [18]. Access-grant tickets may have priority numbers or QoS (Quality-of-Service) values. Watermarked images may have innocence values about their origins in terms of copyright protection. Any product may be associated with insurance contracts [19]. Reward points may be attached. Those values may change unpredictably over time and cause risks. At the worst case, the values get into defaults (*e.g.* the corresponding certificate is revoked) and the holder may have a financial damage (*e.g.* a digital ticket which the holder believes is certified can no longer be used).

A popular way for hedging such stochastic risks is to introduce derivatives or options typically regarding their prices. In financial theory, encouraged by the seminal paper by Black and Scholes [20], option-pricing theories have been developed. Most of them use assumptions including *divisibility* of the underlying assets, which is *not trivial* in the case of the digital objects (suppose, for instance, an object digitally signed by an authority which is not always accessible). Thus we are motivated to study option pricing with models and assumptions suitable for digital objects toward a new risk-management theory in the digital world (a series of its framework appeared in [21, 22]).

C. Concept of VPLs

Suppose that we provide non-trivial technologies and/or theories to solve or improve the security problems. Then the system as a whole is no longer a direct use of VPN. Let us call such a total system as *Virtual Private Laboratories (VPLs).* By using VPLs, researchers in different institutions can get together and cooperate with one another over an open network, and *their research activities are promoted significantly as if they were working in the same laboratories.*

III. DATA-HIDING FOR VPLS

A. Basic Procedures

We consider random data hiding described as follows.

Let $\boldsymbol{y} = (y_1, y_2, \ldots, y_N)^T$ be given measurements or design criteria. Not devoted to a specific data-hiding algorithm, we consider a two-step procedure:

(a) Randomly choose a specified number of the measurements $(y_{j1}, y_{j2}, \ldots, y_{jn})^T$.

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

In the following, n/N is referred to as *density* of this data-hiding. Let us denote the disturbed (*i.e.* watermarked) data by $\boldsymbol{Y}$, and define Signal to Noise Ratio as

$$SNR = 20\log(\|\boldsymbol{y}\| / (\|\boldsymbol{Y} - \boldsymbol{y}\|)). \quad (1)$$

Next, to study inverse estimation in VPLs, we introduce generalized inversion. Let us consider a system equation

$$A\boldsymbol{x} = \boldsymbol{y} \quad (2)$$

where $A = (a_{jj})$ is a system coefficient matrix and $\boldsymbol{y}$ is a given measurement. $\boldsymbol{x} = (x_1, x_2, \ldots, x_M)^T$ is a set of design parameters to be designed by a third party. 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) can not be completely satisfied. In other words, the system

is overdetermined. In this overdetermined case, a generalized-inverse matrix

$$A^+ = (A^T A)^{-1} A^T \qquad (3)$$

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

$$\boldsymbol{x}^+ = A^+ \boldsymbol{y} \qquad (4)$$

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

$$\textit{Minimize}: \|A\boldsymbol{x} - \boldsymbol{y}\|. \qquad (5)$$

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 encounters an overdetermined problem even if M=N; if the client wants to reduce the design components, the number of non-zero parameters may be limited. In designing beamforming arrays, for example, the number of arrays is saved as the solution gets more sparse [23]. Let us suppose that only m(<M) parameters are allowed to be non-zero. In this case, the third party would search for $(i_1, i_2, \ldots, i_m)$ which minimizes the error

$$\|A\_[i_1, i_2, \ldots, i_m]\ (x_{i1}, x_{i2}, \ldots, x_{im}) - \boldsymbol{y}\| \qquad (6)$$

where the coefficient matrix is given by

$$A\_[i_1, i_2, \ldots, i_m] = (\boldsymbol{a}_{i1}, \boldsymbol{a}_{i2}, \ldots, \boldsymbol{a}_{im}) \qquad (7)$$

$$\boldsymbol{a}_{ij} = (a_{1,ij}, a_{2,ij}, \ldots, a_{N,ij})^T. \qquad (8)$$

A random search would be described as follows:

(a) Choose $(i_1, i_2, \ldots, i_m)$ and set the error E to be an infinity.

(b) Compute a minimum-square error solution for $(i_1, i_2, \ldots, i_m)$ as

$$\boldsymbol{x}\_[i_1, i_2, \ldots, i_m]^+ = (0, \ldots, 0, x_{i1}, 0, \ldots, 0, x_{i2}, 0, \ldots, 0, x_{im}, 0, \ldots, 0)^T \qquad (10)$$

where

$$(x_{i1}, x_{i2}, \ldots, x_{im})^T = \mathrm{A}\_[i_1, i_2, \ldots, i_m]^+ \boldsymbol{y}. \qquad (11)$$

(c) If $\|A\boldsymbol{x}\_[i_1, i_2, \ldots, i_m]^+ - \boldsymbol{y}\| < E$, then take the vector $\boldsymbol{x}\_[i_1, i_2, \ldots, i_m]^+$ as a temporary solution and set

$$E = \|A\boldsymbol{x}\_[i_1, i_2, \ldots, i_m]^+ - \boldsymbol{y}\|. \qquad (12)$$

(d) Change $(i_1, i_2, \ldots, i_m)$ randomly and return to (b).

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 (a) or (d)), we solve the square-error problem (Step (b)), and search for better selection (Step (c)).

B. *Effects of Data Hiding (Simulation Setup)*

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 be $\boldsymbol{Y}$ with a density of 0.4.

A *client* entrusts the design to 10 third parties. These parties are called *servers*. The servers are allowed to select at most m=3 non-zero design parameters and search for a better selection by the random search described in the previous section. Each random search is iterated 10 times.

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 a *winner*. By definition, the winner is best in terms of the error for the watermarked data $\boldsymbol{Y}$. 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 could not have such a guarantee in general. This, in turn, motivated us to define an evaluation criterion as follows.

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

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

This procedure is summarized in Fig. 2.

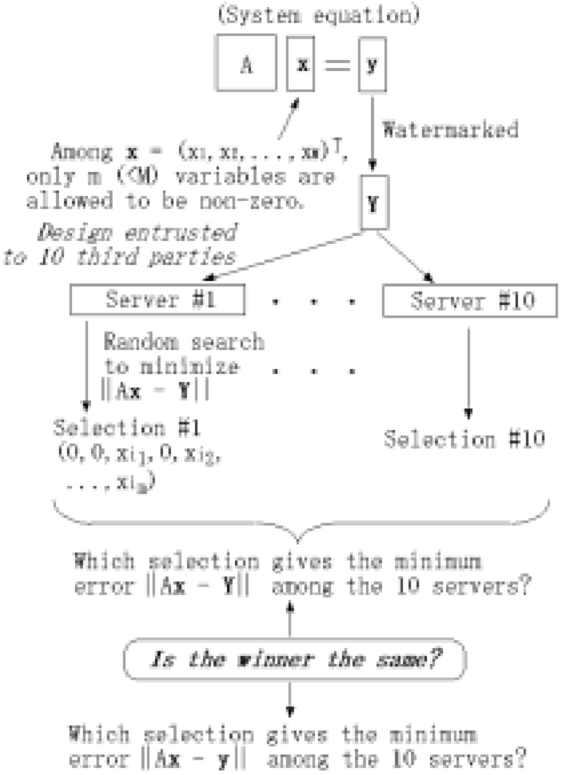


Fig. 2. Design competition among remote servers.

After repeating the procedure, we examined how often the data-hiding was accepted. This rate is defined as the *rate of acceptance* and used as an evaluation criterion.

C. *Effects of Data Hiding (Simulation Result)*

For each set of A and $\boldsymbol{y}$, the simulation is carried out K=100 times. Let the number of acceptance (= how many 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 different by far; one is 1530.4 while the other is 11.97.

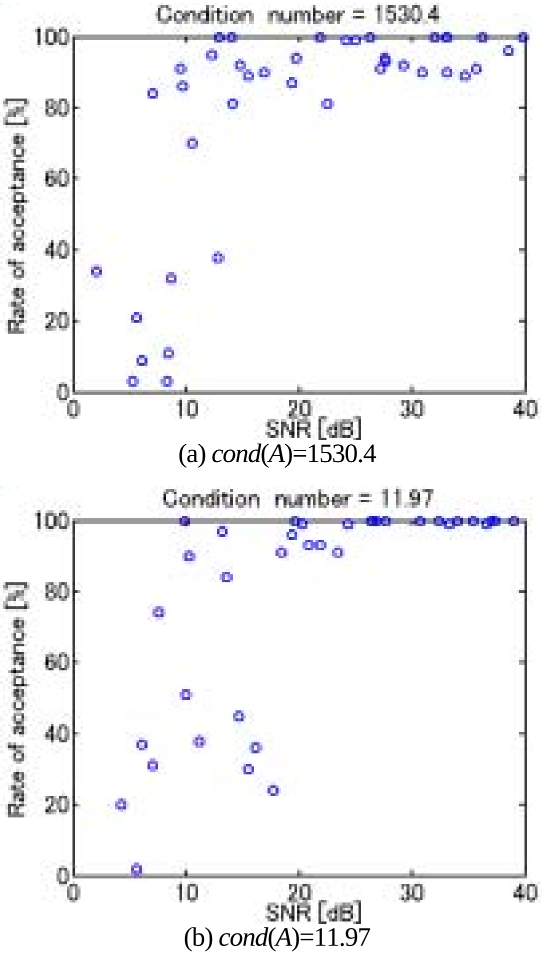
Let us discuss the implication of the simulation results. In linear estimation theory, the condition number of a system coefficient matrix is in close relation to the robustness against errors; larger condition numbers cause larger disturbance. The results in Fig. 3 suggests that

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

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

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

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.



(a) *cond*(*A*)=1530.4

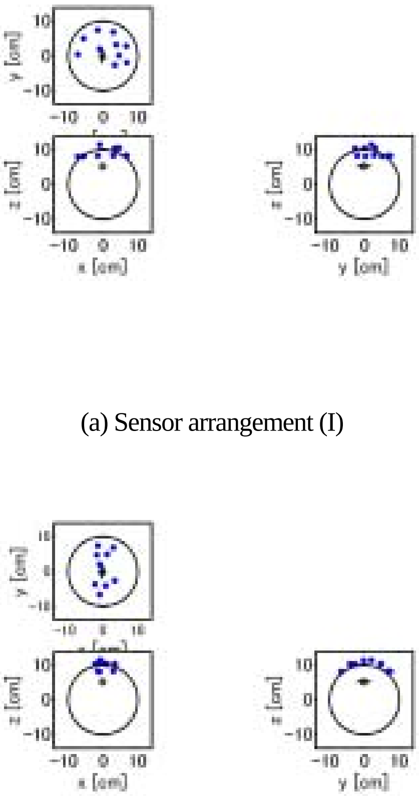
(b) *cond*(*A*)=11.97

Fig. 3. Rate of acceptance vs. Signal-to-Noise Ratio. *cond*(*A*) represents the condition number of system coefficient matrix *A*.

Medical-image processing can be a good application of data-hiding due to privacy issues. For example, in a biomagnetic imaging system, how to determine the active positions in human brain or heart is a fundamental problem [24]. 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 detection-coil types. Our simulation results suggest that the arrangement of the magnetic sensors could be optimized in terms of the robustness against data-hiding.

D. Effects of Data Hiding (Phantom Experiment)

We demonstrate the effect of better condition numbers by using real data measured around a saline-filled spherical phantom whose radius is 10.0cm. 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 an active neural activity by a spiked current dipole. The resultant magnetic signals (magnetic-flux density bandpassed between 0.1-100Hz) were sequentially recorded at N=10 locations. We used two different sensor arrangements shown in Fig. 4. The electrode was located at (-0.11, -0.14, 5.10) [cm] and the manual location error was estimated to be below 0.2cm. 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; the arrangement (I) gives *cond*(*A*)=4.11x10^{10} while the arrangement (II) gives *cond*(*A*)=3.02x10^{9}.



(a) Sensor arrangement (I)

(b) Sensor arrangement (II)

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

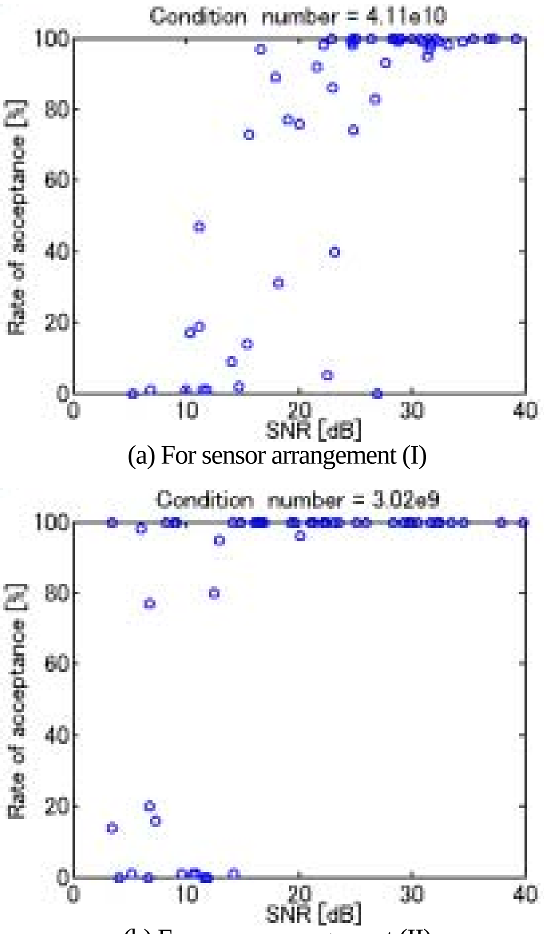
Equally-spaced M=10 grid points (0, 0, 0.5), (0, 0, 1.5), . . ., (0, 0, 9.5) [cm] were set up along z axis in the upper hemisphere (z>0) of the phantom. The current-dipole moments (y-component) at these grid points are design parameters to be determined. We allow two grid points to have non-zero moments 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 the active region along a given sulcus in the brain. The coefficient matrices were computed by using the Biot-Savart law. Then we had a competition similar to that in the former simulation:

(a) The measurement was watermarked with a density of 0.4 and sent to 10 servers.

(b) Each server replied after 10 iterations of the random search.

(c) By changing the watermark 100 times, we obtained the rate of acceptance.

For different SNRs, we obtained rate of acceptance as illustrated 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.



(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 the better robustness.

Let us revisit the conventional idea of watermark evaluation: 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. Our experimental results show *how this conventional evaluation does not work in the case of entrusted data analysis by remote 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 23.3dB. Although this is lower than the threshold SNR found in Fig. 6 (a), conventional human recognition may accept the watermarked image as a good one. By contrast, the latter has an SNR of 35.8dB. Although this is higher than the threshold SNR, human recognition may reject the watermarked image. Thus *the criterion for entrusted data analysis can be different from the conventional one*.

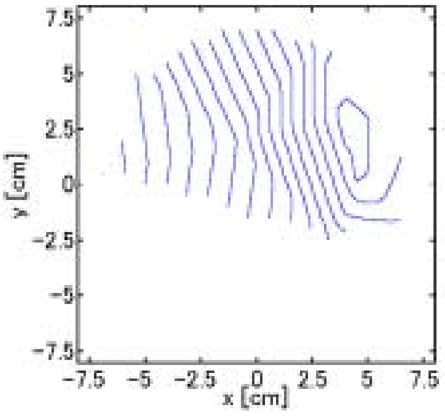


Fig. 6. Contour map of the original magnetic field measured by sensor arrangement (I).

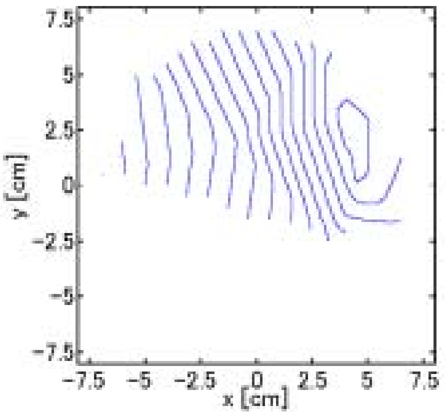


Fig. 7. Contour map of a watermarked magnetic field such that the SNR is 23.3dB.

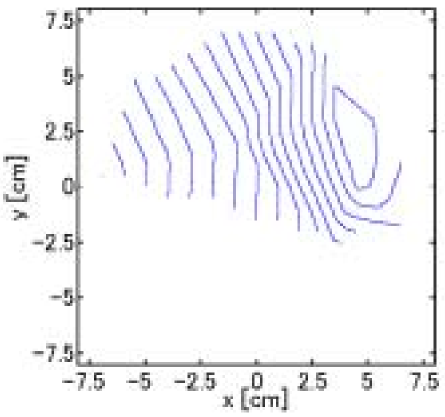


Fig. 8. Contour map of a watermarked magnetic field such that the SNR is 35.8dB.

IV. Concluding Remarks

Aiming at promoting research activities over open networks, this paper introduced a new concept of Virtual Private Laboratories (VPLs) after identifying security problems needed for the activities. The problems include trivial ones and non-trivial ones. With respect to the former, we saw what can be done by a direct use of existing technologies. With respect to the latter, we pointed out two technical building blocks and a new challenge of theory: (1) academic database with multiple security functions, (2) data hiding for the purpose of entrusted data analysis, and (3) risk-management theory for digital objects secured by applied cryptography.

Among the identified problems, this paper studied (2) in detail; the effects of data-hiding were analyzed in the context of entrusted data analysis. Specifically, an entrusted design 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 measured magnetic data in a phantom experiment, and thus we are sure that acceptance criteria for watermarked-and-then-entrusted data can be different from those for conventional watermarked data such as digital images.

We will soon proceed to studies of other building blocks, aiming at implementing a prototype of VPLs.

References

[1] P.W. Dowd and J.T. McHenry, “Network Security: It's Time to Take It Seriously,” *IEEE Computer*, vol. 31, no. 9, pp. 24-28, September 1998.

[2] J.C. Davis, “Protecting Intellectual Property in Cyberspace,” *IEEE Technology and Society Magazine*, vol. 17, no. 2, pp. 12-25, 1998.

[3] K. Matsuura and H. Imai, “Protection of Authenticated Key-Agreement Protocol against a Denial-of-Service Attack,” *Cientifica*, vol. 2, no. 11, pp. 15-19, 1999 [*Digests 1998 Int. Symp. Info. Theory & Its Applications* pp. 466-470, 1998.].

[4] K. Matsuura and H. Imai, “Modified Aggressive Modes of Internet Key Exchange Resistant against Denial-of-Service Attacks,” *IEICE Trans. Info. Sys.*, vol. E83-D, no. 5, pp. 972-979, May 2000.

[5] S. Hamilton, “E-Commerce for the 21st Century,” *IEEE Computer*, vol. 30, no. 5, pp. 44-47, May 1997.

[6] T. Dierks and C. Allen, “The TLS Protocol Version 1.0,” RFC2246, January 1999.

[7] T. Okamoto and K. Ohta, “Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash,” in *Advances in Cryptology --- CRYPTO'89*, Lecture Notes in Computer Science 435, Springer-Verlag, Berlin, pp.481-496, 1990.

[8] D. Chaum and S. Brands, “Minting Electronic Cash,” *IEEE SPECTRUM*, vol. 34, no. 2, pp. 30-34, February 1997.

[9] K.R. Iversen, “A Cryptographic Scheme for Computerized General Elections,” in *Advances in Cryptology --- CRYPTO'91*, Lecture Notes in Computer Science 576, Springer-Verlag, Berlin, pp. 405-419, 1992.

[10] W.A. Arbaugh, J.R. Davin, D.J. Farber and J.M. Smith, “Security for Virtual Private Intranets,” *IEEE Computer*, vol. 31, no. 9, pp. 48-55, September 1998.

[11] E. Kaufman and A. Newman, *Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets*, John Wiley&Sons, 1999.

[12] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC2401, November 1998.

[13] S. Kent and R. Atkinson, “IP Authentication Header,” RFC2402, November 1998.

[14] S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP),” RFC2406, November 1998.

[15] B. Schneier and J. Kelsey, “Secure Audit Logs to Support Computer Forensics,” *ACM Trans. on Information and System Security*, vol. 2, no. 2, pp. 159-176, May 1999.

[16] S. Jajodia, M. Kudo and V.S. Subrahmanian, “Provisional Authorizations,” Chapter 8 in *E-Commerce Security and Privacy*, A.K. Ghosh (ed.), Kluwer Academic Publishers, Boston, 2001.

[17] S. Katzenbeisser and F. Petitcolas (eds.), *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Publishers, Boston, 2000.

[18] M.K. Reiter and S.G. Stubblebine, “Resilient Authentication using Path Independence,” *IEEE Trans. Comput.*, vol. 47, no. 12, pp. 1351-1362, December 1998.

[19] M.K. Reiter and S.G. Stubblebine, “Authentication Metric Analysis and Design,” *ACM Trans. on Information and System Security*, vol. 2, no. 2, pp. 138-158, May 1999.

[20] F. Black and M. Scholes, “The Pricing of Options and Corporate Liabilities,” *Journal of Political Economy*, vol. 81, pp. 637-654, 1973.

[21] K. Matsuura, “Digital Security Tokens and Their Derivatives,” in *7th International Conference of the Society for Computational Economics (SCE'01)*, New Haven, CT, June 2001.

[22] K. Matsuura, “A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce,” in *Proceedings of Third International Conference on Information and Communications Security (ICICS'01)*, S. Qing, T. Okamoto and J. Zhou (Eds.), Lecture Notes in Computer Science 2229, Springer-Verlag, Berlin, pp.90-94, November 2001.

[23] R.M. Leahy and B.D. Jeffs, “On the Design of Maximally Sparse Beamforming Arrays,” *IEEE Trans. Antennas Propagat.*, vol. 39, no. 8, pp. 1178-1187, 1991.

[24] K. Matsuura and Y. Okabe, “Selective minimum-norm solution of the biomagnetic inverse problem,” *IEEE Trans. Biomed. Eng.*, vol. 42, no. 6, pp. 608-615, June 1995.