Regular Paper

An Artifact-metric System Which Utilizes Inherent Texture

Hiroyuki Matsumoto,[†,†††] Itsuo Takeuchi,[†] Hidekazu Hoshino,[†]
Tsugutaka Sugahara[†] and Tsutomu Matsumoto[††,†††]

We have studied on such an authentication system that statistically verifies intrinsic patterns from inherent texture of an individual artifact. Magnetic micro-fibers, which are scattered randomly throughout the substrate of an artifact, form inherent texture of magnetic property. We have found that this inherent texture can be used for *clone* prevention. FibeCrypt is an *artifact-metric* system which examines and authenticates artifacts using both an intrinsic pattern from the inherent texture and a pre-stored reference data protected by a digital signature. In this paper we expound schemes and features of FibeCrypt, and then detail the stored-value card system to which we have applied FibeCrypt. We illustrate results of performance tests for the system. According to our evaluation for the accuracy of authentication of the system, the equal error rate (EER) is 1.5×10^{-4} without retrying. We estimate the accuracy of authentication when we apply a retrying sequence or a double-check scheme. Finally, we describe how to evaluate security of the system, and then discuss, based on the EER, security against a brute force attack by using samples of intrinsic patterns and recorded data. Security against cloning intrinsic patterns is also examined.

1. Introduction

Security technology for protection against cloning valuable documents such as banknotes, passports, tickets, cards, etc., has been advanced. However, while formal publication can be easily done with tools which are now commonplace for the desktop publishing (DTP), the forged documents which are produced with the digital copying techniques, i.e., “*digifeits*,” have recently posed a great threat to document security[11]. Although optically variable devices (OVDs) have been introduced, as an effective measure, for preventing *digifeits*, some imitation banknotes have been detected, which contain such high quality foil that they can deceive the general public. Such high-tech cloning has stimulated research and/or extension efforts on document security.

We have used the term, “*clone*,” to mean the thing which was produced by dishonest ways such as counterfeiting, alteration, duplication, simulation or substitution. Generally, difficulty in producing a *clone* of security feature depends upon its manufacturing processes which involve an expensive machine, a specialized precision technique, a minute tool or the capability to perform a delicate process. In addition, most of security features utilize a uniform device which is applied to each artifact. However, such a feature will not keep its security, provided that an attacker has enough financial power and/or techniques to overcome these hurdles. Accordingly, we have focused on other security features of which security is based on difficulty not in manufacturing processes but in reproducing intrinsic patterns created randomly on each artifact. This concept originated in tampering detection of specific items for intelligence and arms control application[10]. We have proposed such individual authentication systems that authenticate intrinsic patterns randomly created on an artifact can be categorized as *artifact-metric* systems[6].

Various types of *artifact-metric* systems have been proposed and are mainly found in patent literature. Some have utilized intrinsic patterns of optical property by capturing with a photodetector or CCD-array. Inherent texture of small optically reflective particles which are dispersed randomly throughout each artifact has been used for the intrinsic patterns[10]. Random transparency, or translucency, of artifact's substrate was proposed[4]. One utilizes inherent texture of short pieces of plastic optical fiber scattered randomly[9]. Another system employs a nonwoven three-dimensional and random arrangement of polymer fibers[12]. Some have utilized intrinsic patterns of magnetic property by capturing with a magnetic sensor. Inher-

[†] Information & Security Systems Division, NHK Spring Co., Ltd.
[††] Graduate School of Environment and Information Sciences, Yokohama National University
[†††] Graduate School of Engineering, Yokohama National University

ent texture of coated fibers with a magnetic or magnetizable material was proposed to be used for the intrinsic patterns[1]. Furthermore, variation in a magnetic waveform which is called "jitter" has been used[3),14]. Random orientation of magnetic vectors produced by magnetic ink printing has been studied for the intrinsic patterns[5]. Beside these, one has utilized intrinsic patterns of resonant property by sensing metal-fibers with a micro-wave sensor[13].

It is virtually impossible for us to reproduce a sandbox as each grain in the box has the same shape, is the same size, is placed in the same position, etc., as original one. Similarly, it is difficult to produce a perfect *clone* of the inherent texture which was created randomly throughout an artifact, if the texture is investigated down to the minutest details. Therefore, because uniqueness of fine-grained inherent texture can be conclusive evidence of genuineness, intrinsic patterns from the inherent texture provide a great potential for *clone* prevention. Accordingly, we have developed not magnet-coated but magnet-rich micro-fibers to achieve the high level of uniqueness, and then applied to an *artifact-metric* system which we call "FibeCrypt☆ [7),8]." The main reason why we have employed magnetic property is that magnetic property is considered to be more stable against a stain or blot than optical one. This system examines and authenticates an artifact using intrinsic patterns from fine-grained inherent texture of thin magnetic micro-fibers.

While many *artifact-metric* systems have been proposed, most of them are merely conceptual designs or in a development stage. At this point, a handful of the systems has just started to be put to practical use. So, little is known about their practical procedures when applying them to actual applications. In particular, it has not been clear how we can evaluate performance of the systems. Therefore, we would like to give a detailed description of how to apply our system to practical use. The purpose of our study is to clarify how to evaluate security of such a system that statistically verifies intrinsic patterns to authenticate an individual artifact.

In this paper we detail the schemes and features of FibeCrypt. Also, we illustrate the stored-value card system to which we apply FibeCrypt. Finally, we present results of performance tests and discuss security of the system.

2. *Artifact-metric* Systems

2.1 *Artifact-metric* Systems

The goal of *clone* prevention is to provide a level of assurance that an artifact was produced by a proper procedure, by a proper issuer, and that no tampering has occurred in the artifact. We have proposed that "*artifact-metric* systems" can be an effective measure for *clone* prevention[6]. The definition of *Artifact-metric* System is as follows;

An automated system capable of:

(1) capturing an intrinsic pattern sample from an artifact;

(2) extracting an intrinsic feature from that sample;

(3) comparing the intrinsic feature data with that contained in one or more reference templates;

(4) deciding how well they match; and

(5) indicating whether or not an identification or verification of identity has been achieved.

Figure 1 shows the principle of the *artifact-metric* system. The system captures intrinsic patterns which each artifact possesses. After a preprocessing process, the system extracts an intrinsic feature from the patterns, and then classifies the feature as genuine or not using a reference data (template). The reference data must be generated and should be stored in a storage unit on the artifact or in a database (classification dictionary) of the system previous to identification or verification.

2.2 Intrinsic Patterns

The requirements of the intrinsic patterns in the *artifact-metric* systems are as follows.

(1) *Uniqueness*: The intrinsic patterns must be unique to each artifact. In other words, it must be possible to distinguish the intrinsic patterns of a given artifact from the intrinsic patterns of another.

(2) *Permanence*: The intrinsic patterns must be permanent and durable.

(3) *Recognizability*: The intrinsic patterns must be recognizable to the naked eye, or with the use of equipment or devices.

(4) *Clone Resistance*: The intrinsic patterns must be extremely difficult to *clone* or regenerate.

Integrity of the intrinsic patterns, which can

☆ FibeCrypt is a registered trademark of NHK Spring Co., Ltd.

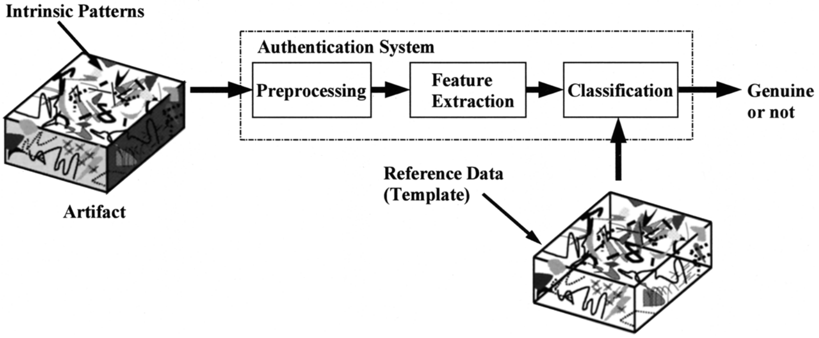


Fig. 1 The principle of the *artifact-metric* system.

be proven by comparing with the reference data, provides conclusive evidence that the artifact has not been tampered with.

3. FibeCrypt

3.1 Fundamental Principle

Inherent texture of magnetic property can be created by scattering magnetic micro-fibers randomly throughout an artifact. We have utilized this inherent texture and developed an *artifact-metric* system which we call FibeCrypt. As shown in **Fig. 2**, FibeCrypt is comprised of an artifact within which magnetic micro-fibers are dispersed randomly, the micro-fibers detector which is a kind of magneto-resistive heads and an authentication procedure. The artifact moves through and is authenticated while being scanned by the micro-fibers detector, provided that the reference data is previously recorded in an issuing procedure.

3.2 Micro-fibers

To acquire clear and stable intrinsic patterns from artifacts, we have developed micro-fibers containing iron oxide particles at the rate of around 70 wt.%. The particles are soft magnetic and thus inhibit attackers from observing them with a conventional magnet viewer. Additionally, both wet and dry types of micro-fibers are available to facilitate various manufacturing processes. The diameter and length of fiber are, for example, respectively around 0.03 mm and 5 mm. Here, the dimensions of fibers are adjustable to fit artifacts in each application. The micro-fibers are so thin that we can apply FibeCrypt to document security. The micro-fibers enable us to make thin (e.g., 50 μm) sheets by combining them with other fibers such as polyethylene terephthalate (PET) fibers, acrylic fibers or cellulose, to utilize our micro-fibers. **Figure 3** (a) shows that each black micro-fiber has a rugged surface and is entangled three-dimensionally itself with other transparent fibers (PET fibers/acrylic fibers). Figure 3 (b) is a microscopic photograph of a

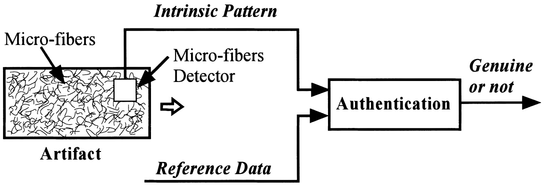
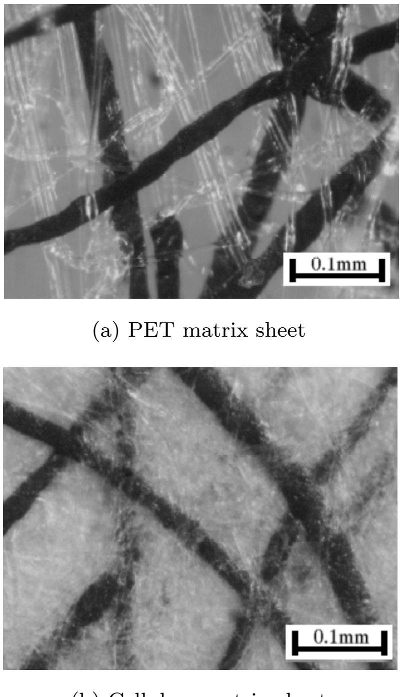


Fig. 2 FibeCrypt utilizes magnetic inherent texture which was created by magnetic micro-fibers.



(a) PET matrix sheet

(b) Cellulose matrix sheet

Fig. 3 The microscopic photographs of micro-fibers sheets.

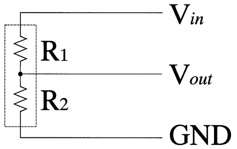


Fig. 4 The equivalent circuit of the micro-fibers detector.

cellulose matrix sheet with micro-fibers. Thus the micro-fibers sheets can be used as inside layers of document substrate by being laminated or coated. The micro-fibers can be either visible or not according as they should be overt or covert in each application.

3.3 Micro-fibers Detector

The micro-fibers detector is a kind of magneto-resistive heads and has two sensor elements. The equivalent circuit of the detector is illustrated in **Fig. 4**. If the input voltage is V_{in}, and the resistances of the sensor elements are respectively R_1, R_2, then the output voltage, V_{out}, is given by

$$V_{out} = V_{in} \times R_2 / (R_1 + R_2) . \qquad (1)$$

Here, the resistance of the i-th sensor element R_i, $i = 1,\ 2$, is given by:

$$R_i = R \times \left(1 + G_i \cdot B_i^2\right) , \qquad (2)$$

where B_i is the magnetic induction of the i-th sensor element, R is the initial resistance of the sensor element, and the geometrical factor G_i which depends upon the element geometry of the i-th sensor element. Each one of the resistances, R_1 and R_2, independently varies when its applied magnetic field is changes. Therefore, as an artifact is scanned, the detector senses magnetic property of the artifact and outputs signals V_{out} according to the variation of R_1 and R_2.

3.4 Authentication

The micro-fibers detector outputs an analog continuous signal according to inherent texture of magnetic property while scanning an artifact. **Figure 5** shows a waveform from the detector. FibeCrypt authenticates the signal, i.e., intrinsic pattern, from the detector through the following processes, i.e., preprocessing, feature extraction and classification.

Preprocessing: The signal is pre-processed by filters, amplifiers and mixers to obtain a manageable and noiseless signal, and then converted to crude data $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$, where c_i, $i = 1, 2, \ldots, n$, represents i-th crude data, by an analog-digital converter with a certain sampling rate. The crude data is stored redundantly to achieve stable authentication and modified by adjusting a gain and offset level to suppress fluctuation noise which is mainly caused by the dispersion of circuit constants and temperature dependency of circuit devices. The system removes glitches with a weighted moving averaging method in order to suppress rapid noise. Finally, the system adjusts a reference edge of verification and quarries, with encoder's pulses, a reference span for verification suppressing mainly velocity fluctuation due to a friction feed.

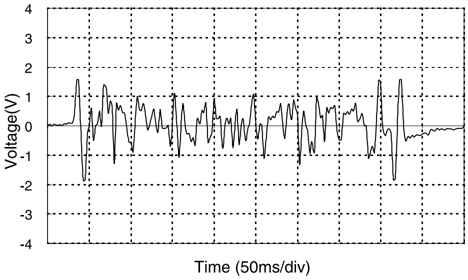


Fig. 5 A waveform from the micro-fibers detector.

Feature extraction: The system extracts, from the crude data $\boldsymbol{c}$, distinctive features, $\boldsymbol{v} = v_1, v_2, \ldots, v_m$, where v_j, $j = 1, 2, \ldots, m$, represents the feature of the block j and is given by:

$$v_j = \sum_{i=h_j}^{k_j} c_i, \qquad (3)$$

where h_j, k_j, are respectively the minimum and maximum ordered number in the j-th block, under the conditions as follows; $h_1 = 1$, $h_j = k_{j-1} + 1$, $j = 2, 3, \ldots, m$, $k_m = n$. The system converts and compresses the data $\boldsymbol{v}$ into the pattern data, $\boldsymbol{p} = (p_1, p_2, \ldots, p_m)$, where p_j, $j = 2, 3, \ldots, m$, represents the pattern data of block j and is given by:

$$p_j = \beta v_j \qquad (4)$$

where β, $0 < \beta \leq 1$, is the constant in compression and depends upon the storage capacity of the recording media in each application.

Classification: The system checks the pattern in an authentication procedure to which we apply a pattern matching scheme based on the correlation coefficient to the authentication of artifacts. Every time the system examines an artifact, pattern data $\boldsymbol{p}' = (p'_1, p'_2, \ldots, p'_m)$ can be extracted from the artifact. Simultaneously, the reference pattern $\boldsymbol{p} = (p_1, p_2, \ldots, p_m)$ can be obtained from the reference data which are previously recorded. The system calculates a degree of similarity of $\boldsymbol{p}$ and $\boldsymbol{p}'$. We adapt the coefficient of determination, i.e., the square of correlation coefficient, $D(\boldsymbol{p}, \boldsymbol{p}')$ as a criterion of similarity:

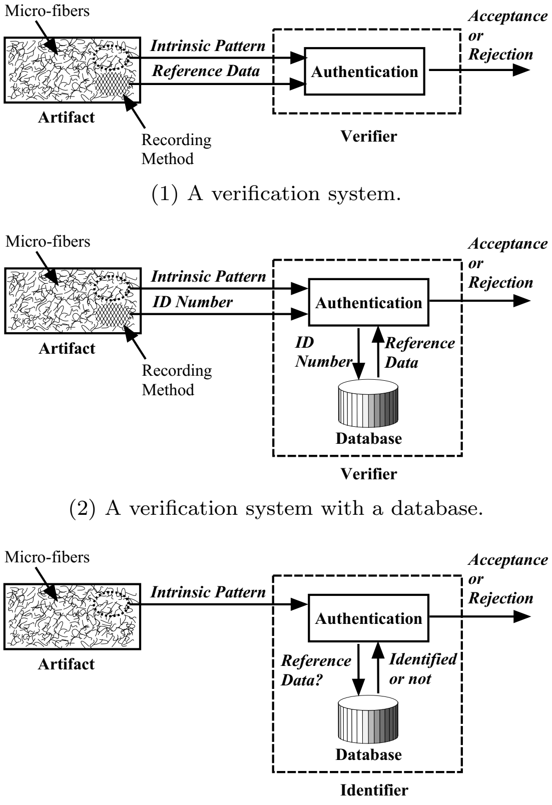
$$D(\boldsymbol{p}, \boldsymbol{p}') = \frac{\left[\sum_{i=1}^{m} (p_i - \bar{p}) \cdot \left(p'_i - \bar{p'}\right)\right]^2}{\sum_{i=1}^{m} (p_i - \bar{p})^2 \cdot \sum_{i=1}^{m} \left(p'_i - \bar{p'}\right)^2}, \tag{5}$$

where $\bar{p}$ and $\bar{p'}$ are mean values of all the elements of the data $\boldsymbol{p}$ and $\boldsymbol{p}'$ respectively. If $D(\boldsymbol{p}, \boldsymbol{p}')$ is greater than or equal to a fixed threshold value, the artifact should be acceptable. Thus the system decides whether the artifact is genuine or not by using its intrinsic pattern.

3.5 Forms of the System

Several forms of FibeCrypt can be available and are similar to those of biometric systems. However, FibeCrypt is distinguished from biometric systems by its availability of recording methods on the subjects. **Figure 6** shows three typical forms.

(1) ***Verification***: Some systems obtain both an intrinsic pattern and a reference data from an artifact, and then verify them. Any recording method such as magnetic stripes, memory chips, bar codes, optical characters and optical marks can be adaptable to the systems. Accordingly, this form enables rather high-speed verification or off-line authentication. The verifier can be a relatively small device because it does not need extra hardware for a database. Therefore, this form fits for instant artifact validation on the spot.



(1) A verification system.

(2) A verification system with a database.

(3) An identification system.

Fig. 6 Three forms of authentication system.

(2) ***Verification with a database***: Some systems look up a reference data in a database by using the identification (ID) number which is recorded on an artifact. Even if there is no recording media on the artifact, ID numbers can be submitted from keypads or some other input devices. Since the database can be located in a remote place and centralized, these systems can immediately void wanted ID numbers when a *clone* is detected.

(3) ***Identification***: The other systems capture an only intrinsic pattern from an artifact and search the reference data which corresponds to the pattern in a database. If the reference data is identified, i.e., exists in the database, the system judges the artifact acceptable. The database in this form also can be located in a remote place. It should be noted that FibeCrypt is an individual authentication system for artifacts, and not for users of them. Therefore, there can be some other forms than those shown in Fig. 6, if it is necessary to authenticate the users. However, it is beyond the scope of this paper to illustrate such authentication systems that are combined with individual authentication systems for users, e.g., biometric systems.

3.6 Features of FibeCrypt

The following describes features of FibeCrypt.

Suitability for inspection: If micro-fibers are applied to the artifacts overtly, the general public can easily check the presence of them with the naked eye. As we mentioned in Section 3.5, FibeCrypt can be applied to diverse forms of authentication systems whether they are on-line or off-line. This enables untrained public to perform instant validation with a verification terminal at each location. In addition, fine-grained inherent texture of thin micro-fibers throughout the body of each artifact can be highly unique enough to provide evidence for professional inspection or forensic use.

Suitability for document substrate:

Because of thin micro-fibers, FibeCrypt can be applied to a variety of artifacts, such as paper documents or plastic cards, with some adjustment in sensitivity of detection, length of scanning, velocity of driving, parameters used in the authentication process, etc. In other words, FibeCrypt provides a substrate document security feature. Generally, substrate document security features such as watermarks or security fibers are considered to be secure against counterfeiting and alteration, as compared with other security features which are printed or attached on the surface of documents.

Reliability: In contrast to security seals, documents circulated are touched by the public and often get soiled by dirt or dust in daily life, such as waste thread, hairdressings, grease or residue of sebaceous matter. They often cause errors in reading and increase the error rates in verification. We have employed the magnetic property which is widely used for recording methods because of its stability against dirt or dust. In addition, we have employed acrylic-fibers in order to increase fold resistance. Thus FibeCrypt is designed to be resistant against rough-handling in daily use.

4. Implementation of the System

4.1 A Stored-value Card System

In this section, we show an application of FibeCrypt for document security. **Figure 7** schematically shows the stored-value card system to which we apply FibeCrypt. This system consists of a stored-value card, a magnetic head, a micro-fibers detector and a controller with a CPU.

The construction of stored-value cards is shown in **Fig. 8**. We laminate thin PET layers (e.g., 75 μm) with other layers on two sides of a micro-fibers sheet. The recording method and physical characteristics of the card are based on the standards of JIS-X-6302 and JIS-X-6311 respectively. In a general application, the additional cost per a card will be around 20% for magnetic stored-value cards. The cost is reasonable and can be lower than that of chip-cards or additional security features such as holograms.

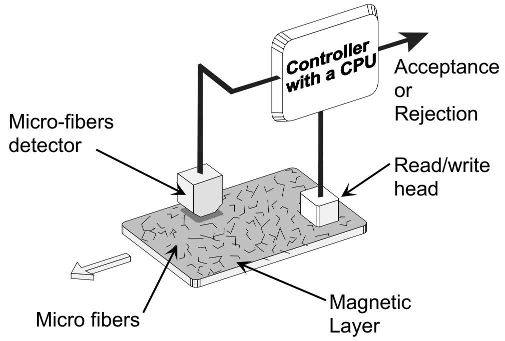


Fig. 7 A stored-value card system.

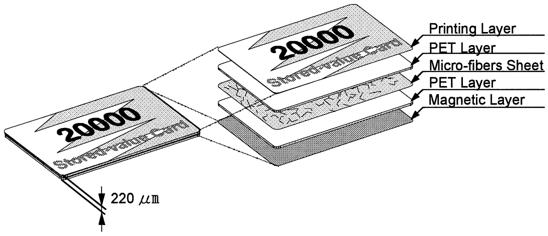


Fig. 8 The structure of the stored-value card.

Table 1 The specification of the card terminal for the stored-value card system.

Card feed	Motor driven (insertion/ejection)
Card feed speed	200 mm/second
Processing time	3.5 second/card (max.)
Life	700,000 card reciprocation
Dimensions	(W) 36.5 mm, (H) 183.4 mm, (D) 147.2 mm
Power source supply	24 $\mathrm{V_{DC}}$ ± 10%, 5 $\mathrm{V_{DC}}$ ± 5%

Table 2 The specification of the encoding machine for the stored-value card system.

Processing speed	2 cards/second (max.)
Card feed speed	200 mm/second
Card hopper capacity	6,000 cards
Dimensions	(W) 2,194 mm, (H) 1,150 mm, (D) 900 mm
Power source supply	100 $\mathrm{V_{AC}}$ ± 10%, (50 Hz/60 Hz)

Before we discuss the accuracy of authentication or security of the system, we must clarify the specifications of the system. We have designed a card terminal and an encoding machine for a stored-value card system. **Table 1** and **Table 2** show the specifications of the card terminal and the encoding machine respectively. Tolerance of the system is shown in **Table 3**. These specifications are so designed as to meet requirements of our customer's system in a practical application. As compared with the card feed speed, from 300 to 400 mm/second, of magnetic PET card readers commercially available, the card feed speed of the card terminal, 200 mm/second, is not high but acceptable.

4.2 Issuing Procedure

First of all, the cards must be encoded its

Table 3 Tolerance of the stored-value card system.

Specifications	Tolerance
Horizontal direction of card movement	±0.75 mm
Vertical direction of card movement	±0.2 mm
Rotational direction of card movement	±10 degrees
Velocity of card movement	100-1000 mm/second

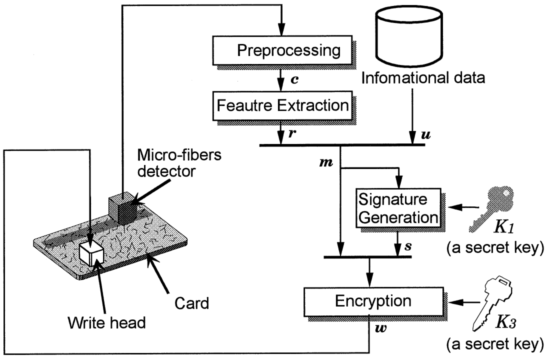


Fig. 9 The flow diagram of the issuing procedure.

reference data in an issuing procedure with an encoding machine. The main purpose of the issuing procedure is to generate a recorded data for each card. The recorded data generally includes a reference data, an informational data and their digital signature. A flow diagram of the issuing procedure which is executed in encoding machines is given in **Fig. 9**. The following describes the issuing procedure.

Step1. [capturing] The micro-fibers detector scans inherent texture of magnetic micro-fibers of the card, and outputs a signal.

Step2. [preprocessing] As shown in Section 3.4, the signal is pre-processed and then converted into crude data $\boldsymbol{c}$.

Step3. [feature extraction] Also, as shown in Section 3.4, the system extracts distinctive features $\boldsymbol{v}$ from $\boldsymbol{c}$, and then converts $\boldsymbol{v}$ into a pattern data $\boldsymbol{p}$.

Step4. [adding information] The system concatenates the reference data $\boldsymbol{r}$, here $\boldsymbol{r} = \boldsymbol{p}$, and an informational data $\boldsymbol{u}$ such as an expiring date, a face value and a place of issue to make a message $\boldsymbol{m}$.

Step5. [signature generation] An asymmetric (public key) signature scheme is applied to generate a digital signature $\boldsymbol{s}$ which corresponds to the message $\boldsymbol{m}$, with a key K_1.

Step6. [encryption] The message $\boldsymbol{m}$ and the signature $\boldsymbol{s}$ are linked, and then are encrypted by a symmetric (secret key) block cipher with a key K_3 to a recorded data $\boldsymbol{w}$.

Step7. [recording] Finally, the recorded data $\boldsymbol{w}$ is written onto the card with the write head.

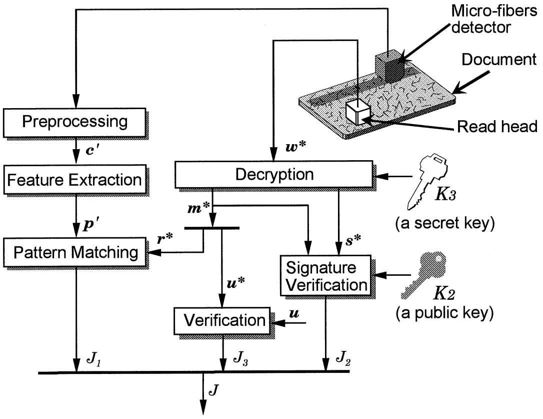


Fig. 10 The flow diagram of the authentication procedure.

4.3 Authentication Procedure

A flow diagram of the authentication procedure which is executed in the card terminals is given in **Fig. 10**. The authentication procedure determines if a submitted card should be accepted or not. The authentication procedure consists of five steps shown below.

Step1. [decryption] A recorded data $\boldsymbol{w}^*$ is read from the magnetic layer with a read head. A message $\boldsymbol{m}^*$ and a signature $\boldsymbol{s}^*$ are extracted by decrypting the recorded data $\boldsymbol{w}^*$. In this paper, we use a superscript asterisk to mean that it may have been changed from the original.

Step2. [data extraction] A reference data $\boldsymbol{r}^*$ and an informational data $\boldsymbol{u}^*$ are simultaneously extracted from the message $\boldsymbol{m}^*$.

Step3. [pattern generation] While the reference data $\boldsymbol{r}^*$ is obtained, a pattern data $\boldsymbol{p}'$ is newly acquired from the card. The pattern data $\boldsymbol{p}'$ is obtained by the same processes as those, from Step 1 to Step 3 in the issuing procedure.

Step4. [discrimination] The pattern matching procedure which we detailed in Section 3.4, is executed in order to verify the pattern data $\boldsymbol{p}'$ with the reference pattern $\boldsymbol{p}^*$, here $\boldsymbol{p}^* = \boldsymbol{r}^*$. Hence, the coefficient of determination $D(\boldsymbol{p}^*, \boldsymbol{p}')$ can be calculated. If $D(\boldsymbol{p}^*, \boldsymbol{p}') \geq \alpha$, here α, $0 \leq \alpha \leq 1$, is the threshold value, then let J_1 be "Acceptance," otherwise let J_1 be "Rejection."

Step5. [signature verification] The message

$\boldsymbol{m}^*$ can be authenticated by checking the signature $\boldsymbol{s}^*$ with a public key K_2. If the message $\boldsymbol{m}^*$ is authenticated, then let J_2 be "Acceptance," otherwise let J_2 be "Rejection."

Step6. [authentication] If both J_1 and J_2 are "Acceptance," and J_3 from verification of the informational data $\boldsymbol{u}^*$ is also "Acceptance," then let the total judgment J be "Acceptance," otherwise let J be "Rejection."

4.4 Cryptography

FibeCrypt utilizes a digital signature scheme in the signature generation and its verification, and a block cipher in the encryption and decryption respectively. We can apply a digital signature scheme such as RSA[☆1], DSA[☆2], an elliptic curve signature scheme, etc. On the other hand, we can apply a block cipher such as DES[☆3], MULTI[☆4], MISTY[☆5], etc. The system has relatively short processing time for the signature generation, the signature verification, the encryption and decryption. The capacity of the memory area and the program required for the configuration of an algorithm have been actualized in the form of size and speed that can be incorporated into the card terminal. Selection of a given constant in the system allows us to form a multifarious cryptosystem.

The security of the digital signature is based on the difficulty in solving a computational problem such as factoring a large number or computing a discrete logarithm over a large finite group. Consequently, the digital signatures guarantee integrity of the recorded data, and thus prevent the intrinsic patterns of the cards from counterfeiting or alteration. There is a synergistic effect of inherent texture and cryptography on security of the system. Intrinsic patterns from the inherent texture protect the system against the *dead copied* cards which are produced by copying the recorded data of a genuine card to another without any change. The intrinsic patterns also protect the recorded data against counterfeiting or alteration.

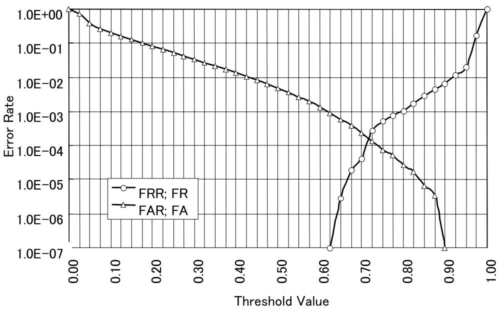


Fig. 11 The accuracy of authentication of the stored-value card system.

4.5 The Accuracy of Authentication

We have examined the accuracy of authentication of the stored-value card system of which specifications are shown in Section 4.1. We have checked the stability of repetitive verification by operating a total of 360,000 times over (600 times over using 200 cards and 3 card terminals). We have also checked the stability of verification by examining responses against other cards a total of 600,000 times over (4,000 times over using 50 stored reference data and 3 card terminals). As a result, the false rejection rate (FRR) and the false acceptance rate (FAR) of the system are shown in **Fig. 11**. For instance, if we set the threshold value to 0.73 corresponding to the equal error rate (EER) where the FRR is equal to the FAR, the system could judge a "not genuine" card as "genuine" and also a "genuine" card as "not genuine" with probability of 1.5×10^{-4}. We obtained this result where length of the pattern data is 96 bits, i.e., 12 sequences of 8 bits (see Section 3.4), and suitable for the rather small capacity of magnetic stripe. Because we could not identify the EER of other *artifact-metric* systems, we have no choice but to compare with biometric systems. For example, the EER of FibeCrypt is lower than the minimum error rate, 1.0×10^{-3}, which is introduced in the ECBS's report for biometric systems [2].

The following part of this section discusses how we can enhance performance of the system based on the accuracy of authentication we obtained in our experiment.

A proper threshold value and a retrying sequence by which the system can verify only once again when the result is "Rejection" on the first try can enhance the performance. If we apply the retrying sequence, the FRR of the system FR_r can be estimated as

[☆1] RSA is a registered trademark of RSA Security Inc.

[☆2] DSA is an acronym for the Digital Signature Algorithm.

[☆3] DES is an acronym for the Data Encryption Standard.

[☆4] MULTI is a trademark of Hitachi Ltd.

[☆5] MISTY is a registered trademark of Mistubishi Electric Corporation.

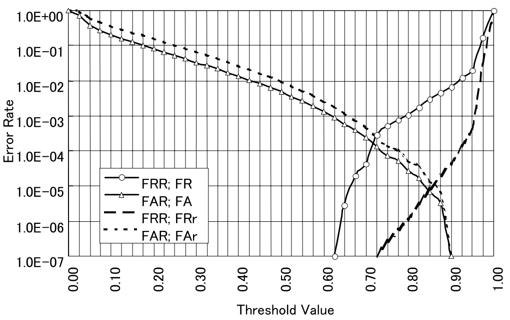


Fig. 12 The accuracy of authentication of the stored-value card system and a calculated effect of the retrying sequence.

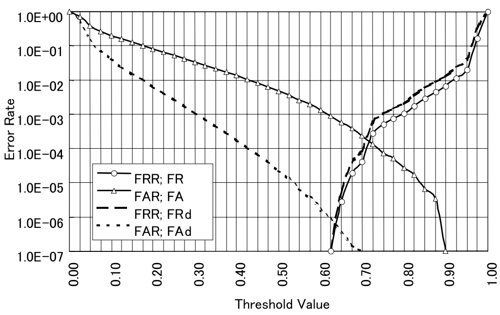


Fig. 13 The accuracy of authentication of the stored-value card system and a calculated effect of the double-check scheme.

$$FR_r = FR^2. \tag{6}$$

The FAR of the system FA_r can be also estimated as

$$FA_r = 1 - (1 - FA)^2 \,. \tag{7}$$

Here, FR and FA are the FRR and FAR of the system without a retrying sequence respectively. We calculated FR_r and FA_r from the experimental result shown in Fig. 11, and show them as the dotted lines in **Fig. 12**. There is a decrease in the EER from 1.5×10^{-4} to 1.1×10^{-5}. We see from this graph that we can enhance performance, i.e., increase the accuracy of authentication, of the system by adjusting the threshold value. Because we always apply the retrying sequence to the system, the actual EER of the system is estimated to be 1.1×10^{-5}.

To meet the requirements of a higher level of security, some parameters in the system can be adjusted to enhance performance of the system. For example, a "double-check" scheme by which the system verifies two intrinsic patterns from two independent textures, and judges "Acceptance" only when both of results are "Acceptance" also can enhance performance of the system. We can estimate the performance in the similar way as the retrying sequence. The FRR of this "double-check" system, FR_d, can be estimated as

$$FR_d = 1 - (1 - FR)^2. \tag{8}$$

The FAR of the double-check system, FA_d, can be also estimated as

$$FA_d = FA^2. \tag{9}$$

Here, FR and FA are respectively the FRR and FAR of the system to which we do not apply the retrying sequence. We calculated FR_d and FA_d from the experimental result shown in Fig. 11, and show them as the dotted lines in **Fig. 13**. There is a decrease in the EER from 1.5×10^{-4} to 4.0×10^{-7}. We see from this graph that we can also enhance performance, i.e., increase the accuracy of authentication, of the system by adjusting the threshold value.

5. Security Evaluation

This section illustrates several ways to deceive card terminals of the system, and then discusses security against a so-called brute force attack using samples of inherent textures and recorded data. We also discuss security against cloning intrinsic patterns.

5.1 Attacks on Card Terminals

Figure 14 diagrammatically shows how to be accepted by a card terminal. In the authentication procedure, a *Verifier* (i.e., a verification terminal) checks *Physical Evidence* (i.e., an intrinsic pattern) with *Logical Evidence* (i.e., a recorded data), and then judges a *Class* (i.e., "Acceptance" or "Rejection"). A recorded data and an intrinsic pattern are obtained by using a sampled data or by producing a data, and by using a sampled texture or by producing a texture respectively. Furthermore, means of producing a recorded data can be put into the five categories in Fig. 14. Means of producing a texture can be also put into the three categories in the same diagram. Therefore, an attack against a card terminal could be executed by presenting a combination of a recorded data and an intrinsic pattern. To deceive the terminal, attackers must procure both a valid intrinsic pattern and a valid recorded data. Here, the valid intrinsic pattern means the pattern which can be processed into a pattern data in the authentication procedure described in Section 3.4. Simultaneously, the valid recorded data means the recorded data which consists of a reference data

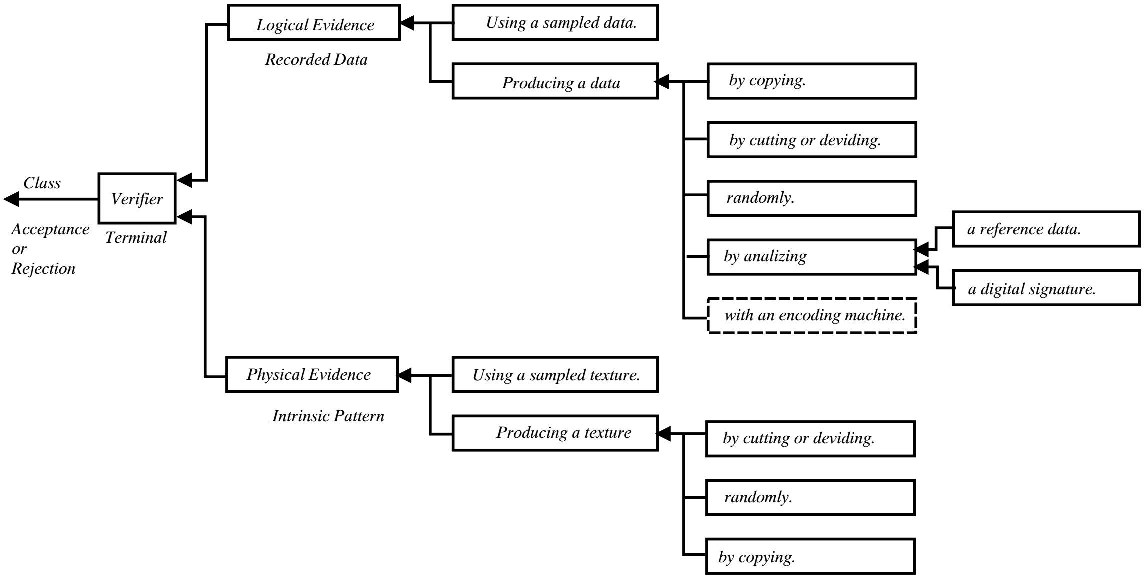


Fig. 14 The diagram of means to be accepted by a card verification terminal.

consistent with a valid pattern, and a digital signature consistent with this reference data.

Of course, genuine cards can be accepted by the terminal because they possess both a valid intrinsic pattern and a valid recorded data. As a result, stolen or lost genuine cards can be also accepted, but this is not our concern in the following discussion.

5.2 Security against a Brute Force Attack

Let us assume that

(1) The reference data are protected by a cryptosystem and enough secure against analyzing,

(2) Attackers cannot tamper with card terminals to analyze an intrinsic pattern, and

(3) Attackers cannot use an encoding machine or secret information about the issuing procedure.

Because the magnetic recording method has become popular, it is reasonable to assume that attackers can read, write or modify a recorded data. On the assumptions, (1) and (3), however, it is difficult for attackers to generate a proper digital signature which is consistent to a given intrinsic pattern, reference data or message. Therefore, there is almost no hope that attackers will succeed in producing a valid recorded data. While it is as much as attackers can do to produce a valid recorded data by a fluke, they can more efficiently collect valid recorded data from cards in circulation and store into a database, and then use them to attack the system. We should think that the recorded data which an attacker uses in her/his attack is always valid when we examine security against attacks on the card terminals.

As we mentioned in Section 3.3, intrinsic patterns depend upon parameters such as magnetic induction, initial resistance and geometrical factors of sensor elements. On the assumptions, (2) and (3), therefore, it is difficult for attackers to know the parameters, where the sensor scans, what intrinsic patterns are, how inherent texture should be, etc. Consequently, it is difficult for attackers to produce a valid inherent texture which is consistent with a given valid recorded data. On the other hand, attackers may reuse cards or may illegally obtain non-recorded cards with micro-fibers. Furthermore, even if they can obtain only micro-fibers, we must consider that they can produce non-recorded cards with micro-fibers. We should think that the intrinsic pattern which an attacker uses in her/his attack is always valid when we examine security against attacks on the card terminals.

In the end attackers can procure valid intrinsic patterns and valid recorded data separately. Accordingly, they may succeed to deceive a card terminal by trying, one by one, with a valid recorded data and a valid pattern. The following discusses security of card terminals against such kind of attacks, namely, a brute force attack.

Let us assume that both valid intrinsic patterns $\boldsymbol{p}_i^v$, $i = 1, 2, \ldots, N_1$, which are members of the finite group of valid intrinsic patterns, $\boldsymbol{X}_{\boldsymbol{p}}^v$, and valid recorded data, $\boldsymbol{w}_i^v$, $i = 1, 2, \ldots, N_2$, which are members of the finite group of valid recorded data, $\boldsymbol{X}_{\boldsymbol{w}}^v$, are distributed random enough. Also, assume that N_1 and N_2 are large enough. To deceive a card terminal by a brute force attack, if an attacker collects $n_1 \geq 1$ samples of valid intrinsic patterns, $\boldsymbol{p}_j^s \in \boldsymbol{X}_{\boldsymbol{p}}^v$, $j = 1, 2, \ldots, n_1$, and samples of valid recorded data, $\boldsymbol{w}_j^s \in \boldsymbol{X}_{\boldsymbol{w}}^v$, $j = 1, 2, \ldots, n_2$, the success rate of the attack, $P(n_1, n_2)$, can be recursively given by

$$P(n_1, 1) = 1 - (1 - FA)^{n_1} \tag{10}$$

and

$$\begin{aligned} &P(n_1, n_2) \\ &= P(n_1, n_2 - 1) \\ &\quad + \{1 - P(n_1, n_2 - 1)\} \cdot P(n_1, 1), \end{aligned} \tag{11}$$

where FA is the false acceptance rate of the terminal. From Eqs. (10) and (11), we can derive

$$\begin{aligned} &P(n_1, n_2) \\ &= P(n_1, 1) \\ &\quad + \{1 - P(n_1, 1)\} \cdot P(n_1, n_2 - 1) \\ &= P(n_1, 1) \\ &\quad + \sum_{k=1}^{n_2-1} \{P(n_1, k+1) - P(n_1, k)\} \\ &= P(n_1, 1) \\ &\quad + P(n_1, 1) \sum_{k=1}^{n_2-1} \{1 - P(n_1, 1)\}^k \\ &= 1 - \{1 - P(n_1, 1)\}^{n_2} \\ &= 1 - (1 - FA)^{n_1 \cdot n_2}. \end{aligned} \tag{12}$$

Consequently, we find that

$$P(n_1, n_2) = P(n_1 \cdot n_2, 1), \tag{13}$$

and also that

$$P(n_1, n_2) = P(n_2, n_1). \tag{14}$$

By this last equation, we can see that the success rate $P(\cdot, \cdot)$ depends upon the product of the numbers of samples, i.e., the number of attacks, $n_1 \times n_2$. We can examine security against a brute force attack by calculating the success rate,

$$P_{n_s} = 1 - (1 - FA)^{n_s}, \tag{15}$$

where $n_s = n_1 \cdot n_2$.

Figure 15 shows the success rate of a brute force attack for the system when we calculate by using Eq. (15) and the results of the EER described in Section 4.5. Assuming that the threshold value in the authentication procedure is set as the FAR is equal to the EER, the three curves, "without retrying," "with retrying" and "with double-check," are calculated for the FARs, $FA = 1.5 \times 10^{-4}$, 1.1×10^{-5} $(= FA_r)$ and 4.0×10^{-7} $(= FA_d)$, respectively.

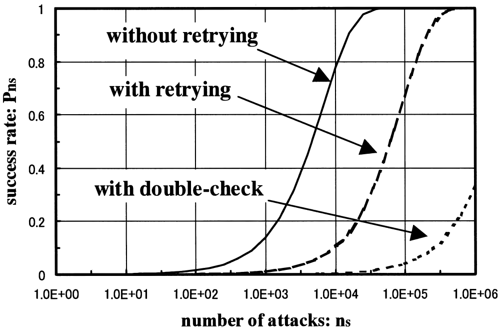


Fig. 15 The success rate of a brute force attack.

Please note that, as we described in Section 4.5, the success rate P_{n_s} can be estimated more decreased than that of "without retrying" because we always apply a retrying sequence to the system. Therefore we examine security of the system when applying the retrying sequence. We can see from the curve of "with retrying" in this graph, to take the case of $n_s = 1.0 \times 10^5$, the success rate P_{n_s} can be nearly equal to 0.67. In this case, it takes around 14 hours when the worst comes to the worst for the attacker to succeed with the probability of 0.67, even if s/he can perform the authentication process at the same speed, i.e., 0.5 second per attempt, as that of encoding machines (see Table 2). This rate may be thought to be rather insecure. But, we think that it is secure enough in such a stored-value card application in which the maximum value of card is limited to 20,000 yen. Furthermore, each card is generally protected by more than ten intrinsic patterns, e.g., each 2,000 yen is protected by one intrinsic pattern. This means that attackers need to determine to do such a work to gain no more than 2,000 yen. Consequently, we consider that attackers rarely try such a waste work. In this way, we can evaluate security and whether the system fits an actual application.

If we apply a "double-check" scheme, we can estimate security in the same way. To take the case of $n_s = 1.0 \times 10^5$, the success rate P_{n_s} can be nearly equal to 0.04. In this case, it takes around 14 hours when the worst comes to the worst for the attacker to succeed with the probability of 0.04. Please note that this is without a retrying sequence. In this way, we

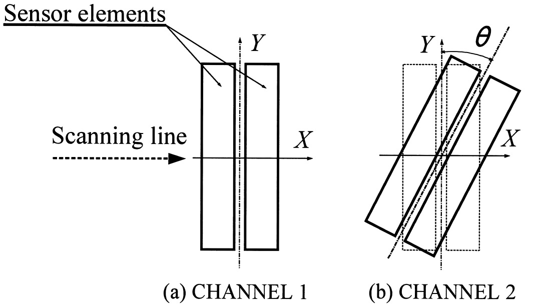


Fig. 16 The difference in geometry between two pairs of sensor element of the two-channel detector.

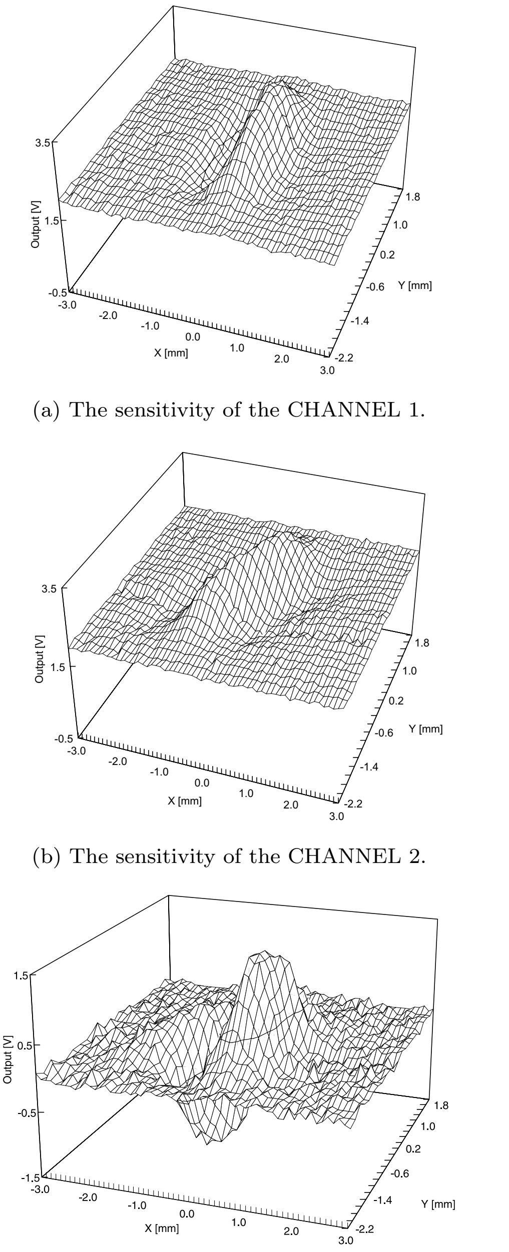
can enhance security of the system to meet a higher level of security requirement.

5.3 Security against Cloning Intrinsic Patterns

In Section 5.2, we discussed the security of the system assuming that attackers cannot tamper with card terminals to analyze an intrinsic pattern. However, if attackers can get a card terminal and observe a signal, i.e., an intrinsic pattern, from the micro-fibers detector, they may produce inherent texture which outputs the similar intrinsic pattern, by using some magnetic materials or its substitutes. As we can see from Eq. (5), attackers can deceive the system if they can achieve $D(\boldsymbol{p}, \boldsymbol{p}') \geq \alpha$ ($0 \leq \alpha \leq 1$; the threshold value in verification) by suppressing errors in reproducing the inherent texture, intrinsic pattern or pattern $\boldsymbol{p}'$. Thus *clone* resistance of intrinsic patterns is crucial for security of the system as well.

We have studied possible ways to enhance security against cloning intrinsic patterns [7),8)]. For example, multi-dimensional detection of inherent texture by using multi-channel detectors will provide a higher level of security. The basic of the multi-channel detector is shown in **Fig. 16** in the case of two channels. The detector is equipped with two pairs of sensor elements which have different geometry/position against the scanning line. The pair of sensor elements (CHANNEL 2) is positioned at the rotation angle θ with another (CHANNEL 1).

The graphs in **Fig. 17** illustrate the sensitivity of a micro-fibers detector. These results are obtained when a spot of magnetic ink is automatically shifting, and directing parallel to the scanning line, under the multi-channel detector (the diameter of the spot is 0.9 mm, the velocity is 200 mm/second). The graph in Fig. 17 (a) shows the sensitivity of CHANNEL 1 in its detectable area. As we can see from this graph, it is probable that changes in the position of magnetic material will still yield the same output voltage, no matter what the element geometry. This means that attackers may simulate an output signal from the micro-fibers detector by putting magnetic material at a certain position. The graph in Fig. 17 (b) shows the sensitivity of CHANNEL 2 in the case of $\theta = 30$



(a) The sensitivity of the CHANNEL 1.

(b) The sensitivity of the CHANNEL 2.

(c) The difference of the sensitivity between CHANNEL 1 and CHANNEL 2.

Fig. 17 The sensitivity of the two-channel detector.

degrees. The graph in Fig. 17 (c) shows differential output of the detectors, CHANNEL 1 and CHANNEL 2. We see from Fig. 17 (c) that each pair of elements has peculiar sensitivity in its detectable area. Thus an output signal from a pair of sensor elements differs from the other, when magnetic material is directed under the detector. This means that changes in the position of magnetic material will change the output signals from both channels. Therefore, to produce a *clone* of inherent texture, attackers must arrange micro-fibers exactly or place magnetic material at a definite geometry/position. It will turn out that the attackers encounter difficulties when they try to produce a *clone* of intrinsic pattern from the texture.

6. Conclusions

Magnetic micro-fibers, which are randomly dispersed throughout each artifact, form inherent texture of magnetic property and can be used for *clone* prevention. FibeCrypt authenticates an artifact by verifying an intrinsic pattern from this inherent texture. In this paper we detailed the schemes and features of FibeCrypt, and then illustrated a stored-value card system to which we have applied FibeCrypt. We examined the accuracy of authentication of the system, and discussed security against brute force attacks using samples of inherent textures and recorded data. A retrying sequence and a "double-check" scheme are useful to enhance security of the system. Also, we discussed security against cloning inherent texture. How we clarify *clone* resistance of intrinsic patterns is a question to be answered and what we might go on to.

In this paper we have discussed a stored-value card system. While, generally in stored-value card applications, it is not necessary to authenticate card users, other applications such as ID card applications require not only *clone* prevention of cards but also individual authentication of users. From the standpoint of individual authentication of users of artifacts, there can be multifarious forms of the system that are combined with other systems such as biometric systems. The future direction of this study will be on a more detailed security evaluation for the multifarious forms of the system.

Acknowledgments The authors are grateful to all members who have been working on FibeCrypt.

References

1) Brosow, J.: Document having fibers which are coated with a magnetic or magnetizable material embedded therein and an apparatus for checking authenticity of the documents, US patent 4,114,032 (1978).

2) ECBS: *Biometrics: A Snapshot of Current Activity*, European Committee for Banking Standards (1996).

3) Fernadez, A.J.: Data Verification Method and Magnetic Media Therefor, US patent 5,235,166 (1993).

4) Goldman, R.N.: Non-counterfeitable Document System, US patent 4,785,290 (1988).

5) Hayosh, T.D.: Self-Authentication of Value Documents, *Proc. SPIE*, Vol.3314, pp.140–149 (1998).

6) Matsumoto, H. and Matsumoto, T.: Artifact-metric systems, Technical Report of IEICE, No.ISEC2000-59, pp.7–14 (2000).

7) Matsumoto, H., Yamamotoya, K. and Matsumoto, T.: Document Protection by Micro-Fibers and Cryptography, *Proc. PISEC '99* (1999).

8) Matsumoto, H., Suzuki, K. and Matsumoto, T.: A clone preventive authentication technique which features magnetic micro-fibers and cryptography, *Proc. SPIE*, Vol.3314, pp.275–286 (1998).

9) National Material Advisory Board: *Commission on Engineering and Technical Systems, National Research Council, Counterfeit Deterrent Features for the Next-Generation Currency Design*, pp.74–75, National Academy Press (1993).

10) Poli, D.L.: Security Seal Handbook, Technical Report, Sandia National Laboratory (1978).

11) van Renesse, R.L.: Synagestic combination of document security techniques, *Proc. SPIE*, Vol.3973, pp.126–138 (2000).

12) van Renesse, R.L.: 3DAS: A 3Dimensional-stracture Authentication System, *European Convention on Security and Detection* (1995).

13) Samyn, J.: Method and Apparatus for Checking the Authenticity of Documents, US patent 4,820,912 (1989).

14) Watanabe, Y., Kobara, K. and Imai, H.: Examining the security of cryptosystems based on the difficulty of forging random parameters, Technical Report of IEICE, No.ISEC97-9, pp.85–94 (1997).

(Received December 12, 2000)
(Accepted June 19, 2001)

Hiroyuki Matsumoto received the B.E. degree in mechanical engineering from the University of Electro-Communications, Tokyo, Japan, and joined NHK Spring Co., Ltd., Yokohama, Japan, in 1982. He had been engaged in pattern recognition systems, and received the M.E. in electronic information engineering from Toyota Technological Institute, Nagoya, Japan, in 1987. He is currently taking a Ph.D. course at Yokohama National University while working as a manager of the Information & Security Systems Division. His research interests include document security and biometrics.

Itsuo Takeuchi received the B.E. degree in chemical engineering from Yokohama National University, Japan, and joined NHK Spring Co., Ltd., Yokohama, Japan, in 1982. He has been engaged in development of information security systems, and is a manager of the Information & Security Systems Division. His research interests focus on anti-counterfeiting techniques that utilize special optical characteristics.

Hidekazu Hoshino received the B.E. degree in electrical engineering from Science University of Tokyo, Japan, and joined NHK Spring Co., Ltd., Yokohama, Japan, in 1980. He had been engaged in image processing and pattern recognition systems. He has worked as a leader in research and development of anti-counterfeiting techniques, and has invented several security products. He is currently a chief manager in the engineering department of the Information & Security Systems Division.

Tsugutaka Sugahara received the B.E. degree in mechanical engineering from Hosei University, Tokyo, Japan, in 1972. In 1973, he joined NHK Spring Co., Ltd., Yokohama, Japan, and then had been engaged in development of printers and card readers/writers. He is the senior manager of the Information & Security Systems Division, which he has developed as a new business unit in NHK Spring Co., Ltd. since 1987, and has been working on anti-counterfeiting devices, access control systems and other security systems.

Tsutomu Matsumoto was born in Maebashi, Japan, on October 20, 1958. He received the Dr. Eng. degree from the University of Tokyo in 1986, and since then his base has been in Yokohama National University where he is enjoying research and teaching in the field of cryptography and information security as a Professor in Graduate School of Environment and Information Sciences. He is a member of Cryptography Research and Evaluation Committee of Japan. He served as the general chair of ASIACRYPT 2000. He is an associated editor of Journal of Computer Security, and was on the board of International Association for Cryptologic Research and the Japan Society of Security Management. He received Achievement Award from the IEICE in 1996.