Regular Paper

Clone Match Rate Evaluation for an Artifact-metric System

Hiroyuki Matsumoto† and Tsutomu Matsumoto††

We have examined magnetic *artifact-metric* systems, which authenticate an artifact by verifying intrinsic patterns from magnetic texture randomly created on it. Also, we have illustrated how to efficiently evaluate the accuracy of authentication for a magnetic *artifact-metric* system. In this paper we produce *clones* using a magnetic material in accordance with acquired signals from the magnetic texture on a genuine artifact, and then measure the acceptance rates of them for the magnetic *artifact-metric* system. Based on our experimental results, we reveal that the *clone* match rates (CMRs) do not always depend on the original false match rates (FMRs). Therefore, we should evaluate the CMRs of the system using possible *clones* when we examine security of *artifact-metric* systems.

1. Introduction

A recent trend in counterfeiting is "casual counterfeiting" with easily available tools and materials, such as for desktop publishing. The spread of casual counterfeiting by non-professional counterfeiters has stimulated research and/or extension efforts on security of valuable documents, such as banknotes, passports, tickets, cards, etc.

Individual authentication of each document by verifying its physical characteristic potentially achieves a secure anti-counterfeiting system. Accordingly, we have studied such individual authentication systems that authenticate intrinsic patterns from magnetic texture randomly created on documents [9),10)]. The first thing we did in the study was to research other studies for similar systems, which utilize intrinsic patterns of artifacts for authentication. These patterns are extracted from, for example, optical images of distributed fibers [15),19)], micro-wave signals from random arrangement of metal fibers [16)], magnetic signals from magnetizable fibers [4)], jitter in reading and writing processes [6)], or random orientation of magnetic vectors [7)]. Based on the research, we systematized them as *artifact-metric* systems [11),12)]. Subsequently to the systematization, we have evaluated performance of a magnetic *artifact-metric* system, and proposed an efficient way of performance evaluation [13),14)].

Generally, individual authentication systems are applied to authentication of artifacts or persons along the following lines:

(1) Individual authentication of an artifact is done
  (a) by verifying/identifying physical characteristics of the artifact (e.g., *artifact-metric* systems), and/or
  (b) by verifying/identifying logical characteristics of the artifact (e.g., magnetic/chip card systems).
(2) Individual authentication of a person is done
  (a) by verifying/identifying physical characteristics of the person (e.g., biometric systems using fingerprints, irises, or hand shapes),
  (b) by verifying/identifying behavioral characteristics of the person (e.g., biometric systems using handwritings, or gaits),
  (c) by verifying/identifying logical characteristics of the person (e.g., access control systems using knowledge of passwords), and/or
  (d) by individual authentication of an artifact which the person possesses, verifying relation between the artifact and the person.

Artifact-metric systems are analogous to biometric systems in the respect that they verify intrinsic patterns from physical objects. Biometric systems are often said to be convenient, being as they need no portable tool such as a card. To put it the other way around, biometric features are inseparable from the users, and

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

☆ This work was done when the first author was a Ph.D. student in Graduate School of Engineering at Yokohama National University.

therefore difficult to replace with substitutes even if they were counterfeited. In this view, *artifact-metric* systems are inferior in convenience and however superior in replaceability, to biometric systems. A further important point is that *artifact-metric* systems have an advantage over biometric systems in ability to be enhanced for their accuracy of authentication by adjusting physical characteristics.

We have used the term "*clones*" to mean those things, which are produced by methods such as counterfeiting, alteration, duplication or simulation. Even as we have examined performance of the magnetic *artifact-metric* system, security evaluation against *clones* has been still open. In general, security evaluation for individual authentication systems against attacks using *clones* has been rarely disclosed. Designers or sellers of the systems would not like to make public *clone* resistance of their technique, telling their customers that they cannot give the details of security architecture of the technique on behalf of its security. They may insist that the technique is physically protected by difficulty in its manufacturing processes, which involve an expensive machine, a specialized precision technique, a minute tool or the capability to perform a delicate process. Also, they may insist that the technique is logically protected by cryptography. However, such a technique will not keep its security, assuming that an attacker has enough financial power, insider information, and/or techniques to overcome these hurdles. As a matter of fact, some researchers have pointed out vulnerability of chip cards [1),2),8)]. Others have also pointed out vulnerability of fingerprint systems against *clones* [17),18)]. *Artifact-metric* systems remain secure as a consequence of inevitable difficulty in reproducing random patterns, even if an attacker overcome the hurdles. Therefore, the primary consideration in evaluation of *artifact-metric* systems should be given into security against attacks using *clones*.

The purpose of this paper is to evaluate security of a magnetic *artifact-metric* system against *clones*. We produce *clones* with magnetic materials using a programmable industrial robot. We compare the acceptance rates for the *clones* with the original accuracy of authentication, which is measured without using *clones*, and then discuss security of the system. In addition, we demonstrate the acceptance rates of the *clones* for the magnetic *artifact-metric* system when changing parameters, e.g. resolution of the intrinsic patterns, in the authentication processes of the system. The evaluation method, which is demonstrated in this paper, will have applicability to other *artifact-metric* systems and also biometric systems.

2. The *Clone* Match Rate

Artifact-metric systems verify intrinsic patterns from physical objects stochastically, and are similar to biometric systems, in which the inevitable errors occur in authentication. Therefore, the accuracy of *artifact-metric* systems can be evaluated with the false non-match rate (FNMR) and false match rate (FMR), which are widely used for performance evaluation of biometric systems [3),20)]. The FNMR and FMR are functions of the decision threshold, which the system applies to its pattern matching algorithm. The FNMR is the rate that an *artifact-metric* system will fail to verify the identity of a legitimate artifact, and the FMR is the rate that the *artifact-metric* system will incorrectly identify an artifact. Furthermore, the equal error rate (EER) is defined as the rate of errors when the decision threshold is set such that the FNMR equals to the FMR, and commonly used as a representative indicator of the accuracy.

Other indicators, i.e. the false rejection rate (FRR) and the false acceptance rate (FAR) have become well-known to public, and are often used as the indicators of the accuracy of authentication for individual authentication systems. We demonstrated that we could improve the accuracy by applying some special protocols, e.g., a multi-check protocol, to the system [14)]. Consequently, we are using the FRR and FAR to refer to the ultimate accuracy regardless of performance enhancement.

In our evaluation we need to incorporate a rate in order to indicate the false match rate for *clones*, and so use the term, "the *clone* match rate (CMR)," to refer to the rate that the *artifact-metric* system will incorrectly identify a *clone*. While the FMR is the match rates for a non-self artifact, the CMR is a special case of the FMR, and indicates the match rate for a *clone* artifact. While practical *artifact-metric* systems usually employ some secure protocols, we examine the system with the primitive indicators, i.e., FMR, FNMR and CMR, in order to eliminate influence of difference in protocols, in this paper.

3. The Target of Security Evaluation

3.1 *F-papers*

In our evaluation, we use paper documents throughout which magnetic micro-fibers, containing iron oxide particles at the rate of 70 wt.%, are randomly dispersed. The diameter and length of fiber are respectively around 0.03 mm and 5 mm. The average density of fibers in a square meter is one gram, and the size is 210×75 mm. We call the paper documents "*F-papers*."

3.2 The Magnetic *Artifact-metric* System

We evaluate security of a magnetic *artifact-metric* system. As shown in **Fig. 1**, the magnetic *artifact-metric* system consists of a magnetic reader and a personal computer (PC). The magnetic reader with a micro-fibers detector scans an *F-paper*. The detector consists of two elements of magneto-resistive sensor, and outputs a differential output signal of the elements. In the magnetic reader, the intrinsic patterns from magnetic texture on the *F-paper* can be captured by the micro-fibers detector, quantized into 256 numbers by an analog to digital converter, and then transferred to the PC via the RS232-type serial interface. The PC authenticates the intrinsic patterns of the *F-paper* by the procedures to which we apply a pattern-matching scheme based on the correlation. The details of the authentication procedures are described in Appendix A.1.

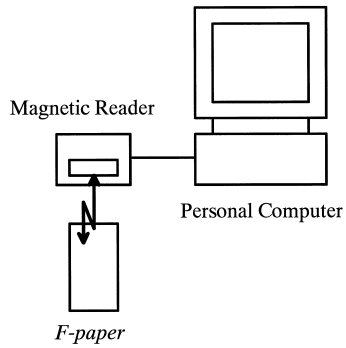


Fig. 1 The magnetic *artifact-metric* system consists of a magnetic reader and a personal computer.

3.3 Authentication of *F-papers*

Figure 2 schematically shows the structure of the magnetic *artifact-metric* system. The authentication of *F-papers* can be achieved by the procedures, i.e., preprocessing, feature extraction and classification. Generally, it is considered to be easier for counterfeiters to control a linear system than other complex systems when they try to make *clones*. We regard the magnetic *artifact-metric* system as a linear system for the purpose of carrying out a security evaluation against casual counterfeiting. In Fig. 2, micro-fibers detector linearly outputs an analog signal $y(t)$ according to an analog input $x(t)$ of a pattern of micro-fibers. In this case, $x(t)$ is considered as a magnetic pattern and also considered to be produced by a discrete magnetic input pattern $x\,[n]$. In the preprocessing process, $y(t)$ is converted into the discrete pattern $y\,[n]$. Since the model is a linear system, $y\,[n]$ can be denoted as a convolution of an input pattern $x\,[n]$ and the impulse response $h\,[n]$ of the detector.

4. How to Attack the System

4.1 Counterfeiters

A non-professional counterfeiter often attacks the system by a simple control method with easily obtainable tools and materials. We think that security evaluation against such a casual attack is crucial for the security of system. In this paper we examine security of the magnetic *artifact-metric* system on the following assumptions.

(1) A counterfeiter can use the magnetic reader.

(2) The counterfeiter can make the same preprocessing unit that is used in the system, and can check the discrete pattern

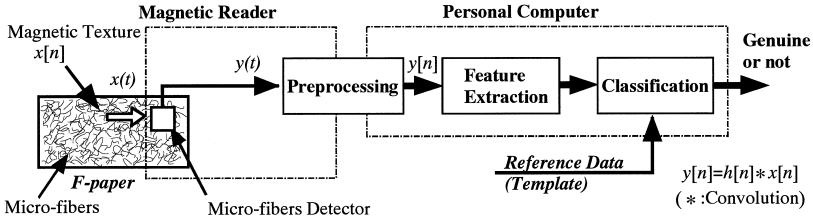


Fig. 2 A linear model is used in the security evaluation against cloning intrinsic patterns.

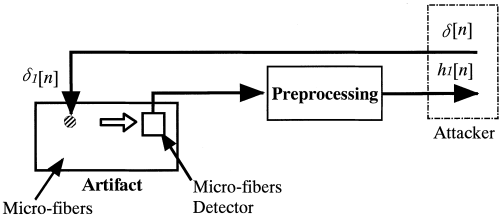


Fig. 3 Acquisition of a pseudo-impulse response.

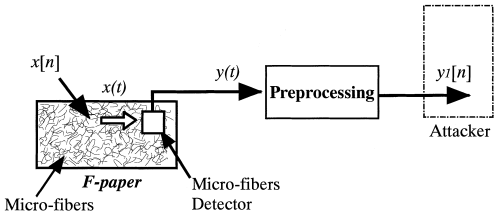


Fig. 4 Acquisition of an example data.

$y[n]$ from *clones* of *F-papers*.

(3) The counterfeiter cannot know what feature extraction and classification are, but can try to deceive the system by using a *clone*.

(4) In the case that the *clone* can be accepted by the computer, the counterfeiter will succeed in the trial.

In the counterfeiting, the counterfeiter obtains both an impulse response of a detector and an example data from a target artifact in order to copy an intrinsic pattern. The following sections detail how to attack the system.

4.2 Acquisition of Responses

Figure 3 schematically illustrate how the counterfeiter acquires a pseudo-impulse response, and then tries to examine a response of the detector by inputting a discrete impulsive function $\delta[n]$ as a desired value. However, the actual discrete input to the detector is not $\delta[n]$ but a pseudo-impulsive function $\delta_1[n]$ because there may be some errors. Thus, the acquired response $h_1[n]$ can be thought as a pseudo-impulse response of the detector.

4.3 Calculation of a Magnetic Pattern

Figure 4 schematically illustrates how the counterfeiter acquires an example data. The counterfeiter can observe a response of the detector while the detector scans an *F-paper*, and obtain an example pattern $\boldsymbol{y}_1 = (y_1[0], y_1[1], \ldots, y_1[N])^t$. An output pattern can be denoted as a convolution of an input data and the pseudo-impulse response, as we mentioned in Section 3. Therefore, the example pattern $\boldsymbol{y}_1$ is supposed to be given by a linear transformation:

$$\boldsymbol{y}_1 = \boldsymbol{h}_1 \cdot \boldsymbol{x}_1. \tag{1}$$

In Eq. (1), $\boldsymbol{h}_1$ is an impulse response matrix derived from the pseudo-impulse response $h_1[n]$ and given by

$$\boldsymbol{h}_1 = \begin{bmatrix} h_1[0] & 0 & \cdots & 0 \\ h_1[1] & h_1[0] & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ h_1[N] & h_1[N-1] & \cdots & h_1[0] \end{bmatrix}. \tag{2}$$

Also, $\boldsymbol{x}_1 = (x_1[0], x_1[1], \ldots, x_1[N])$ is a calculated magnetic pattern. Since the inverse of matrix $\boldsymbol{h}_1^{-1}$ always exists, $\boldsymbol{x}_1$ can be uniquely calculated from $\boldsymbol{h}_1$ and $\boldsymbol{y}_1$ by

$$\boldsymbol{x}_1 = \boldsymbol{h}_1^{-1} \cdot \boldsymbol{y}_1. \tag{3}$$

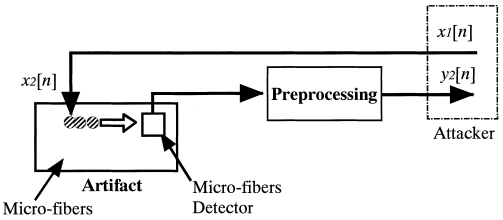


Fig. 5 Reproduction of a magnetic pattern.

4.4 Reproducing a Magnetic Pattern

Copying an intrinsic pattern involves a reproducing procedure, which is schematically shown in **Fig. 5**. The counterfeiter tries to reproduce a magnetic pattern $\boldsymbol{x} = (x[0], x[1], \ldots, x[N])$ by inputting the calculated magnetic pattern $\boldsymbol{x}_1$ as a desired value. However, the actual discrete input to the detector may be not $\boldsymbol{x}_1$, but $\boldsymbol{x}_1$ with some errors, denoted as the pattern $\boldsymbol{x}_2 = (x_2[0], x_2[1], \ldots, x_2[N])$. Finally, the counterfeiter obtains the *clone* pattern $\boldsymbol{y}_2 = (y_2[0], y_2[1], \ldots, y_2[N])^t$.

5. Experiments

5.1 Experimental Apparatus

We use a high precision orthogonal robot with 3 axes, which specification is shown in **Table 1**, to make *clones* of *F-papers*. The robot is a kind of programmable robot for industrial use, such as a high precision dispensing use. We suppose that this kind robot is available even for non-professional counterfeiters, and can be used to make a *clone*. The cloning apparatus, shown in **Fig. 6**, consists of a robot equipped with a needle and its controller. Please note that we use the robot without its additional dispenser

Table 1 Specifications of the robot.

Work range	X: 200 mm, Y: 200 mm, Z: 50 mm
Positioning accuracy	X, Y: $> \pm 0.05$ mm, Z: $> \pm 0.05$ mm
Transporting speed	X, Y: 1–500 mm/sec, Z: 1–200 mm/sec
Resolution	0.0125 mm/pulse
Max. load capacity	5 kg
Interpolation function	Linear & Circular
Program capacity	2,000 steps

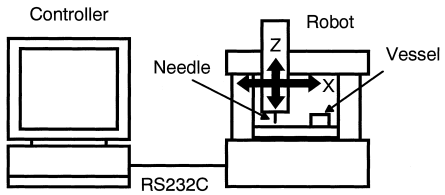


Fig. 6 The cloning apparatus consists of a robot with a needle, and its controller.

function.

Magnetic materials for industrial use and copy papers for copiers are used for producing *clones*. The magnetic materials, which stirred into a water and water-soluble gel mixture, are applied to the material for producing magnetic texture on the *clones*. These materials are commercially available iron oxide particles, and not so difficult even for non-professional counterfeiters to obtain.

Every time the robot receives a command, the robot transfers its needle from the original position to a small vessel, picks up the magnetic material from the vessel with the needle, moves over the paper, and then presses the needle onto the determined positions of paper to mark a dot. The size of the single dot is around less than 0.5 mm when we use the needle of which diameter is 0.3 mm. The reason why we chose this needle is that we can obtain stable results in our preliminary examination with several types of needles. Accordingly, we performed the experiments using this needle as an ideal one that non-professional counterfeiters use to make a *clone*.

The robot automatically marks with a dot of the magnetic material to a position on the paper, according to a control program. Finally, we can produce magnetic texture on a paper by plotting, with the magnetic materials, the control positions, which we can previously calculate.

Figure 7 schematically illustrates how to

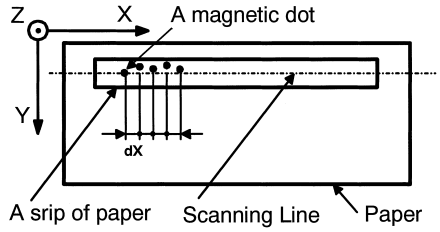


Fig. 7 The robot marks dots on the slip at the fixed interval dX along the scanning line, i.e., X axis. We control the input level by adjusting the distance between the dot and the scanning line, i.e., Y axis.

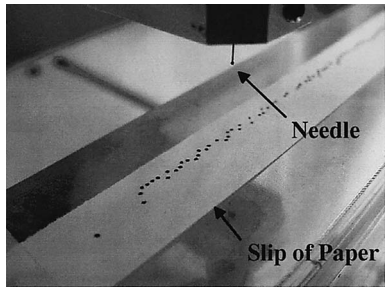


Fig. 8 The robot dots with the magnetic material on a long narrow slip of paper in accordance with the calculated magnetic pattern.

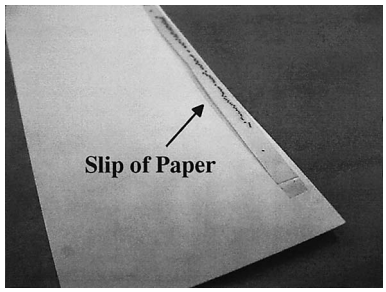


Fig. 9 We attach the slip onto a white paper to make a *clone*.

make a dot on the paper. As shown in **Fig. 8** and **Fig. 9**, we use a slip of paper to mark a dot, and then attach it onto the paper to make a *clone*. The robot marks dots on the slip at the fixed interval dX along the scanning line, i.e., X axis. We control the input level by adjusting the distance between the dot and the scanning line, i.e., Y axis. The transporting speeds for X and Y axes, and Z axis are 100 mm/sec and 50 mm/sec, respectively. These parameters are employed because we can obtain stable results in our preliminary examination. The fixed interval dX is around 0.88 mm. Each *clone* pattern consists of 100 dots of magnetic materials, and therefore its length is around 88 mm.

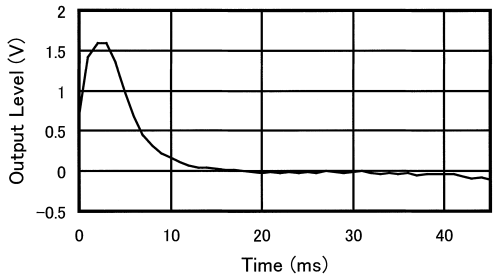


Fig. 10 An example of acquired response $h_1[n]$ when we measure, a single dot which were marked by the robot according to a single command as a discrete impulsive function $\delta[n]$.

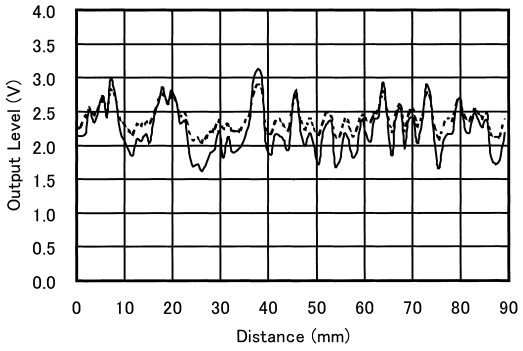


Fig. 11 An example pattern $\boldsymbol{y}_1$ and its calculated pattern $\boldsymbol{h}_1 \cdot \boldsymbol{x}_1$ are indicated by the solid line and the dotted line, respectively.

It is nearly equal to the length that the magnetic reader can stably transport an *F-paper*, and therefore considered to be enough for us to examine the system. The following describes the actual procedures of cloning.

5.2 Acquisition of Responses

A single command given from the robot controller produces a single dot of the magnetic material on a certain position of the paper. We make a single dot marked at the position of the paper, which is just on the scanning line of the micro-fibers detector. The single command corresponds to a discrete impulsive function $\delta[n]$. **Figure 10** shows an example of acquired response $h_1[n]$ when we measure the paper with the single dot. The response was observed from one element of the micro-fibers detector. Finally, we can obtain an impulse response matrix $\boldsymbol{h}_1$ as given by Eq. (2), and then calculate its inverse of matrix $\boldsymbol{h}_1^{-1}$.

5.3 Calculation of a Magnetic Pattern

An example pattern $\boldsymbol{y}_1$ acquired from the one element of the micro-fibers detector in the evaluation is shown in **Fig. 11** as a solid line. As

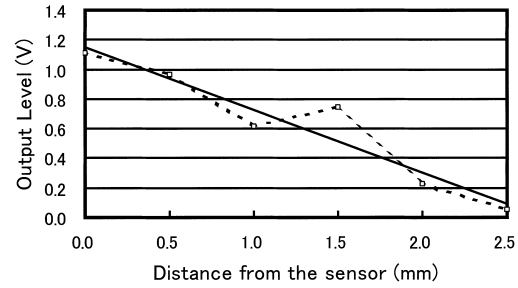


Fig. 12 This figure shows output levels of the detector for the distance between the center of the detector and the magnetic dot.

we have mentioned in Section 3, the pattern $\boldsymbol{y}_1$ is not invariable because of inevitable errors. In order to suppress the errors, we employ an averaged pattern of the patterns acquired in 10 times measurement as the example pattern $\boldsymbol{y}_1$. Although the resolution of the example data is rather high, the robot, which we used in our experiments, cannot reproduce each element of the example pattern because of its marking ability. For that reason, we have no choice but to compress the example pattern by averaging each 50 sequential elements. We redefine the compressed example pattern as the example data $\boldsymbol{y}_1$. Finally, by Eq. (3), we can find a calculated magnetic pattern $\boldsymbol{x}_1$. Figure 11 also shows the pattern $\boldsymbol{h}_1 \cdot \boldsymbol{x}_1$, which is calculated from the example pattern, as a dotted line. We can see from Fig. 11 that $\boldsymbol{h}_1 \cdot \boldsymbol{x}_1$ is not the same as $\boldsymbol{y}_1$. However, the correlation coefficient between these patterns is nearly equal to 1.0.

5.4 Reproducing a Magnetic Pattern

We reproduce a target magnetic pattern $\boldsymbol{x}$ by controlling the robot. The robot is so programmed that it marks sequentially dots with the magnetic material in accordance with the calculated magnetic pattern $\boldsymbol{x}_1$. The control positions of the needle are calculated by a function of $\boldsymbol{x}_1$. This function can be regarded as linear because we found that the sensitivity of the detector is almost linear for the distance between the center of the detector and the single dot, as shown in **Fig. 12**. Finally, we make a *clone* by controlling the robot in accordance with the calculated magnetic pattern $\boldsymbol{x}_1$. **Figure 13** shows an intrinsic pattern obtained from the genuine *F-paper* as a solid line, an intrinsic pattern from its *clone* as a dotted line. Each signal was obtained as a differential output signal from the micro-fibers detector. We can see that the *clone* pattern is similar to the

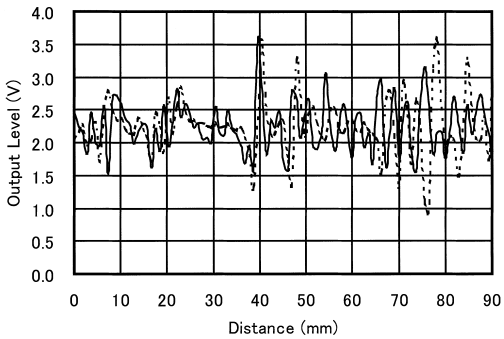


Fig. 13 An intrinsic pattern obtained from the genuine *F-paper* is indicated as a solid line, and an intrinsic pattern from its *clone* as a dotted line.

F-paper's pattern.

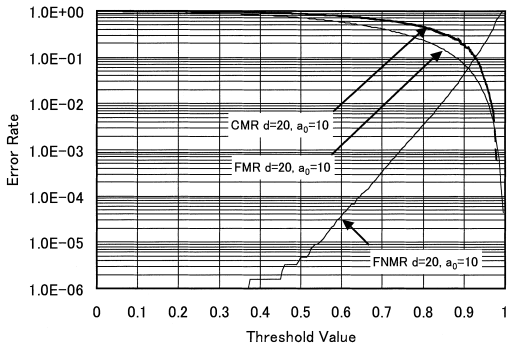
5.5 The Measurement Method

We make *clones* of an *F-paper* by following the above-mentioned procedures. As we mentioned in Section 4, we assume that the counterfeiter cannot know what feature extraction and classification procedures are employed in the system. In our experiment, we measure CMRs of the magnetic *artifact-metric* system without any special protocols. That is to say, we simply use the feature extraction and classification procedures, which are described in Appendix A.1. We examine the system when we set the template as $\boldsymbol{y}_1$, by adjusting d and a_0.

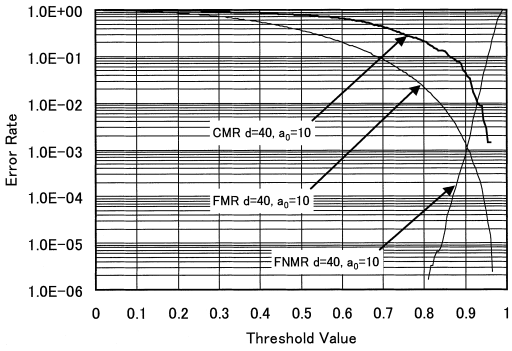
6. Experimental Results

We tried to make 100 *clones* of an *F-paper* by following the above-mentioned procedures for reproducing a target magnetic pattern. We examine the acceptance rates for the *clones*, which we made. The CMRs are shown in **Fig. 14** (a), (b) and (c) when we set the number of elements as $d = 20$, 40 and 80, respectively. In these figures, $d = 20$, 40 and 80 indicate the ranges to be verified, and respectively correspond to around 3.5 mm, 7.0 mm, and 14.0 mm.

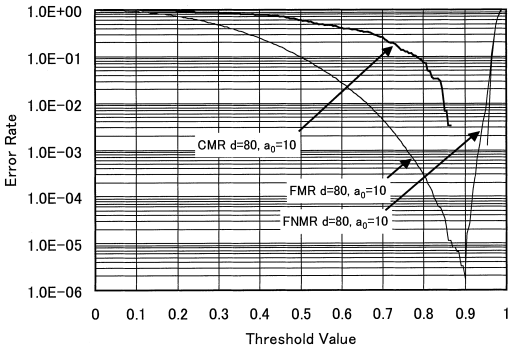
As we can see from Fig. 14, it is clear that the CMRs indicated by thick solid curves are commonly higher, for all the cases, than those of the original FMRs indicated by thin solid curves. For the purpose of comparison, we dare to find the EER for $d = 80$ as around 1.0×10^{-3}. Thus, we can see from the results that the EERs are 1.0×10^{-1}, 1.0×10^{-2} and $\approx 1.0 \times 10^{-3}$, respectively, for $d = 20$, 40 and 80. We can also find that the original EERs for the same verification algorithm are 6.0×10^{-2}, 1.0×10^{-3} and 1.1×10^{-6}, respectively for $d = 20$, 40 and 80, assuming that the presented patterns are not *clones*. As we compare the EERs for *clones* with the original EERs, the FMRs for *clones*, i.e., CMRs, will not be so decreased with an increase in d. The results shown in Fig. 14 were obtained where we sequentially had averaged every 10 elements of raw pattern, i.e., $a_0 = 10$ (see Appendix A.1) to acquire intrinsic



(a) The CMR curve is presented when we set the number of elements as $d = 20$.



(b) The CMR curve is presented when we set the number of elements as $d = 40$.



(c) The CMR curve is presented when we set the number of elements as $d = 80$.

Fig. 14 The CMRs are shown when we set the number of elements as $d = 20$, 40 and 80, respectively. In these cases, we set the resolution as $a_0 = 10$.

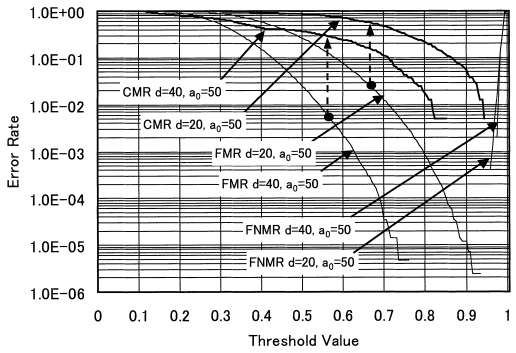


Fig. 15 The CMR curves are presented when we set the resolution for verification as the same resolution, $a_0 = 50$.

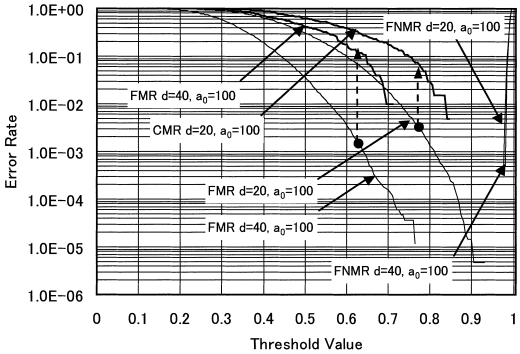


Fig. 16 The CMR curves are presented when we set the resolution for verification as the same resolution, $a_0 = 100$.

patterns.

This resolution for verification is higher than that for positioning the needle in reproduction, and is equivalent to $a_0 = 50$. In order to clarify effects of the resolution on the error rates, we examine the CMRs when we set the resolution for verification as the same resolution, $a_0 = 50$, and its results are shown in **Fig. 15**. In this figure, $d = 20$ and $a_0 = 50$, and $d = 40$ and $a_0 = 50$, correspond to the verification ranges, around 17.5 mm and 35.0 mm, respectively. Also, the results for a lower resolution, $a_0 = 100$, are shown in **Fig. 16**. In this figure, $d = 20$ and $a_0 = 100$, and $d = 40$ and $a_0 = 100$, correspond to the verification ranges, around 35.0 mm and 70.0 mm, respectively. We can see from the figures that the FMRs for *clones*, i.e. CMRs, are higher than the original FMRs in all the cases. Furthermore, we can find, from the results, the following important facts.

(1) As shown in **Fig. 17**, the CMRs are almost the same even if the original FMRs are entirely different from each other.

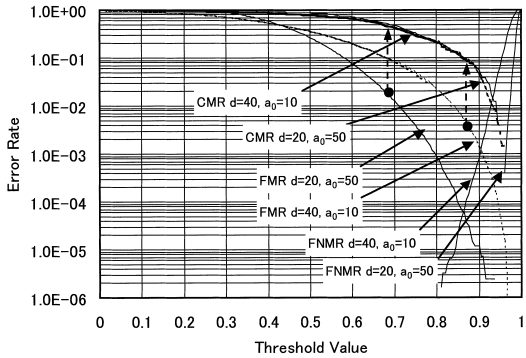


Fig. 17 The CMRs are almost the same even if the original FMRs are entirely different from each other.

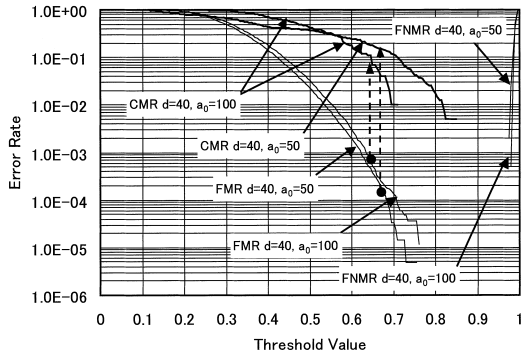


Fig. 18 The CMRs are almost the same or rather reversed, even if the original FMRs are nearly equal to each other.

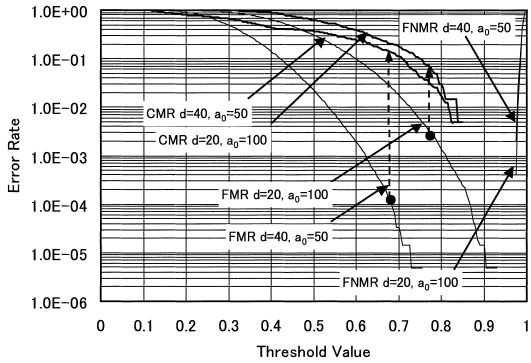


Fig. 19 The results are plotted together, when we set as $d = 40$ and $a_0 = 50$, and $d = 20$ and $a_0 = 100$.

(2) Contrary to this, the CMRs are almost the same or rather reversed, even if the original FMRs are nearly equal to each other, as shown in **Fig. 18**.

(3) **Figure 19** shows, together, the results when we set as $d = 40$ and $a_0 = 50$, and $d = 20$ and $a_0 = 100$. In both cases, the system verifies intrinsic patterns in the

same range, which corresponds to around 35.0 mm, of the *clones*. These are different in resolution for verification. We can see from this graph that the CMRs become close to each other even if the original FMRs are entirely different from each other.

The experimental results in this paper are obtained only for 100 *clones*, and therefore not so precise. However, they are enough for us to know that the CMRs cannot be estimated with the original FMRs.

7. Conclusions

In this paper we have examined security of the magnetic *artifact-metric* system. We demonstrated an actual cloning technique with the tools and materials, which are considered to be available for counterfeiters. We observed the impulse response of the system and example patterns, and then calculated corresponding magnetic patterns. According to the calculated magnetic patterns, we reproduced 100 *clones* controlling a high precision orthogonal robot with 3 axes. While the experiments were performed on the definite conditions and based on the assumption that the system is linear, the methodology used in this paper will be helpful to security evaluation for not only the magnetic *artifact-metric* systems but also other *artifact-metric* systems.

Of course, exact FMRs cannot be easily given where a counterfeiter exists, since the counterfeiter may access to or utilize more precise machinery and more suitable materials in reproduction. However, we think that it is useful to evaluate the system even on a certain definite condition, in order to clarify its security, i.e., capability to prevent *clones*, and to take measures against the *clones*.

Clone resistance of the magnetic *artifact-metric* system was presented as the CMR curves by way of evaluating the acceptance rates of the *clones*. Differences in the accuracy of authentication were also presented when changing the resolution for verification. We examined the magnetic *artifact-metric* system of which EERs are 6.0×10^{-2}, 1.0×10^{-3} and 1.1×10^{-6} for the different resolutions when the presented patterns are not *clones*. In our experiments, we found that these EERs respectively changed to 1.0×10^{-1}, 1.0×10^{-2} and $\approx 1.0 \times 10^{-3}$ for the *clones* that we made. Even if these results were measured without applying any protocols that enhance security, they show that the EER of the system is almost equal to the required error rate, 1.0×10^{-3}, which is introduced in the ECBS's report for biometric systems [5]. In case that we apply this magnetic *artifact-metric* system to a magnetic card system, the card cost will be lower than that of a chip card or of a magnetic card with a hologram as cost increase per a card is around 20%. As it turned out, we will be able to enhance security of the card at a reasonable cost by introducing the system.

The experimental results revealed that the CMRs could not be estimated with the original FMRs. In other words, the CMRs do not always depend on the original FMRs. Consequently, we should evaluate the CMRs of the system using possible *clones* when we examine security of *artifact-metric* systems. This fact also suggests that we should examine security of the biometric systems, which stochastically verify intrinsic patterns of individuals, with the CMR evaluation.

Acknowledgments This research was partially supported by MEXT Grant-in-Aid for Scientific Research on Prioritiy Areas 13224040 (Tsutomu Matsumoto).

References

1) Anderson, R.J. and Kuhn, M.G.: Tamper Resistance — a Cautionary Note, *The Second USENIX Workshop on Electronic Commerce Proceedings*, Oakland, California, November 18–21, pp.1–11 (1996).
2) Anderson, R.J. and Kuhn, M.G.: Low Cost Attacks on Tamper Resistant Devices, *Security Protocols, Proc. 5th International Workshop*, Lomas, M., et al. (Eds.), Paris, France, April 7–9, LNCS 1361, pp.125–136, Springer (1997).
3) ANSI A9.84-2001, Biometrics Information Management and Security (2001).
4) 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, patent number US4114032 (1978).
5) ECBS: Biometrics: A snapshot of Current Activity — 1996, European Committee for Banking Standards, TR400 (1996).
6) Fernadez, A.J.: Data Verification Method and Magnetic Media Therefor, patent number US5235166 (1993).
7) Hayosh, T.D.: Self-Authentication of Value Documents, *Proc. SPIE*, Vol.3314, pp.140–149 (1998).

8) Kocher, P., Jaffe, J. and Jun, B.: Differential Power Analysis, Springer-Verlag, LNCS 1666, pp.388–397 (1999).
9) 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).
10) Matsumoto, H., Yamamotoya, K. and Matsumoto, T.: Document Protection by Micro-Fibers and Cryptography, *Proc. PISEC'99*, Barcelona, Spain (1999).
11) Matsumoto, H. and Matsumoto, T.: Artifact-metric systems, *Technical Report of IEICE*, ISEC2000-59, pp.7–14 (Oct. 2000).
12) Matsumoto, H., Takeuchi, I., Hoshino, H., Sugahara, T. and Matsumoto, T.: An Artifact-metric System Which Utilizes Inherent Texture, *IPSJ Journal*, Vol.42, No.8, pp.139–152 (2001).
13) Matsumoto, H. and Matsumoto, T.: How to Evaluate Accuracy of Authentication for a Magnetic Artifact-metric system, *Technical Report of IEICE*, PRMU2001-160, pp.45–52 (Dec. 2001).
14) Matsumoto, H. and Matsumoto, T.: An Evaluation Method for a Magnetic Artifact-metric System, *IPSJ Journal*, Vol.43, No.08, pp.2458–2466 (2002).
15) National Material Advisory Board: Commission on Engineering and Technical Systems, National Research Council, *Counterfeit Deterrent Features for the Next-Generation Currency Design*, Publication NMAB-472, pp.74–75, National Academy Press (1993).
16) Samyn, J.: Method and Apparatus for Checking the Authenticity of Documents, patent number US4820912 (1989).
17) Yamada, K., Matsumoto, H. and Matsumoto, T.: Can We Make Artificial Fingers That Fool Fingerprint Systems?, *Technical Report of IEICE and IPSJ*, ISEC2000-45, pp.159–166, and Vol.2000, No.68, pp.159–166 respectively, Tokyo, Japan (July 2000).
18) van der Putte, T. and Keuning, J.: Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, *Smart Card Research and Advanced Applications*, IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pp.289–303 (2001).
19) van Renesse, R.L.: 3DAS: A 3Dimensional-structure Authentication System, ECOS95, *European Convention on Security and Detection*, Brighton, UK (1995).
20) Wayman, J.L.: Technical Testing and Evaluation of Biometric Identification Device, *Biometrics: Personal Identification in Networked Society*, Jain, A. K., Bolle, R. and Pankanti, S. (Eds.), The Kluwer Academic, International Series in Engineering and Computer Science, Vol.479, Chapter 17, pp.345–368 (1999).

Appendix

A.1 The Procedures in the System

The followings are a feature extraction procedure, registration, and a classification procedure in the magnetic *artifact-metric* system [13),14)].

A.1.1 Feature Extraction

From the magnetic reader, the PC receives a raw data,

$$\boldsymbol{r} = (r_1, r_2, \ldots, r_n)^t, \tag{4}$$

where $r_i\,(i = 1, 2, \ldots, n)$ represents i-th raw data.

The raw data will be averaged and compressed in order to remove glitches or rapid noises. By sequentially averaging every $a_0 \geq 1$ elements of the raw data $\boldsymbol{r}$, the PC compresses $\boldsymbol{r}$ into the compressed pattern,

$$\boldsymbol{c} = (c_1, c_2, \ldots, c_m)^t, \tag{5}$$

where $c_j\,(j = 1, 2, \ldots, m)$ represents the mean value of the block j, and is given by

$$c_j = \frac{1}{a_0} \sum_{i=(j-1)a_0+1}^{j \cdot a_0} r_i. \tag{6}$$

Finally, by extracting $d\,(1 \leq d \leq m)$ sequential elements of $\boldsymbol{c}$, we can obtain an intrinsic pattern,

$$\boldsymbol{P}_{d,k} = (c_k, c_{k+1}, \ldots, c_{k+d-1})^t, \tag{7}$$

where $1 \leq k \leq m$ and $k + d - 1 \leq m$.

A.1.2 Registration

A template $\hat{\boldsymbol{P}}_{d,r}$, where the subscript r indicates a reference point, i.e. $k = r$, can be created by capturing the intrinsic patterns from the same *F-paper* $M \geq 1$ times. In the magnetic *artifact-metric* system, the PC calculates the template $\hat{\boldsymbol{P}}_{d,r}$ as the average of the intrinsic patterns $\boldsymbol{P}^i_{d,r}$, where the subscript $i = 1, 2, \ldots, M$ indicates the multiple samples from the same *F-paper*. We define a mean value of the k-th elements of $\boldsymbol{P}^i_{d,r}$ as

$$p_k = \frac{1}{M} \sum_{i=1}^{M} c^i_k, \tag{8}$$

where $k = r, r + 1, \ldots, r + d - 1$.

Finally, we can write the template as

$$\hat{\boldsymbol{P}}_{d,r} = (p_r, p_{r+1}, \ldots, p_{r+d-1})^t . \qquad (9)$$

A.1.3 Classification

The PC classifies an *F-paper* whether genuine or not by checking its intrinsic pattern in the subsequent authentication procedure to which we apply a pattern-matching scheme based on the correlation. Every time the PC examines an *F-paper*, a compressed pattern $\boldsymbol{c} = (c_1, c_2, \ldots, c_m)^t$ is captured, and then an intrinsic pattern $\boldsymbol{P}_{d,r} = (c_r, c_{r+1}, \ldots, c_{r+d-1})^t$, will be extracted from $\boldsymbol{c}$. Simultaneously, a template, $\hat{\boldsymbol{P}}_{d,r} = (p_r, p_{r+1}, \ldots, p_{r+d-1})^t$ at the corresponding reference point can be obtained from the templates, which are previously recorded. If we define the degree of similarity between $\boldsymbol{P}_{d,r}$ and $\hat{\boldsymbol{P}}_{d,r}$ as $S(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r})$, which can be calculated as follows:

$$S(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r}) = \frac{\sum_{i=r}^{r+d-1} (c_i - c_r) \cdot (p_i - \bar{p})}{\sqrt{\sum_{i=r}^{r+d-1} (c_i - \bar{c}_r)^2 \cdot \sum_{i=r}^{r+d-1} (p_i - \bar{p})^2}}, \qquad (10)$$

where $\bar{c}_r$ and $\bar{p}$ are mean values of all the elements of the patterns $\boldsymbol{P}_{d,r}$ and $\hat{\boldsymbol{P}}_{d,r}$, respectively. Actually, in the classification process, the intrinsic pattern is captured redundantly to compensate for position errors of the reference point. Every time the PC examines an *F-paper*, $(2s + 1)$ redundant patterns $\boldsymbol{P}_{d,(r-s)}$,$\boldsymbol{P}_{d,(r-s+1)}$, …,$\boldsymbol{P}_{d,r}$, …, $\boldsymbol{P}_{d,(r+s-1)}$,$\boldsymbol{P}_{d,(r+s)}$, where $s \geq 0$ is the number of shifts, will be extracted from $\boldsymbol{c}$. The PC calculates the minimum value of $S(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r})$ by

$$S_{\min}(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r}) \stackrel{def}{=} \min_{-s \leq k \leq s} S(\boldsymbol{P}_{d,(r+k)}, \hat{\boldsymbol{P}}_{d,r}), \qquad (11)$$

where the value of the reference point r is limited as $s + 1 \leq r \leq m - d - s + 1$.

Finally, the PC classifies the *F-paper* as acceptable, i.e., genuine, if $S_{\min}(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r}) > \alpha$, otherwise not, according to a fixed threshold value, α.

(Received November 29, 2002)
(Accepted June 3, 2003)

Hiroyuki Matsumoto received the B.E. degree in mechanical engineering from the University of Electro-Communications, and joined NHK Spring Co., Ltd. in 1982. He received the M.E. degree in electronic information engineering from Toyota Technological Institute in 1987, and the Ph.D. degree in artificial environment and systems from Yokohama National University in 2002. Presently, he serves on the program committee of Optical Security and Counterfeit Deterrence Techniques V in Electronic Imaging 2004. His research interests include document security and biometrics.

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 the Cryptography Research and Evaluation Committees of Japan. He served as the general chair of ASIACRYPT 2000. He is on the board of International Association for Cryptologic Research. He is a member of IEICE Technical Group on Information Security and of IPSJ Special Interest Group on Computer Security. He received Achievement Award from the IEICE in 1996.