Analysis of Brute-Force Break-Ins of a Palmprint Authentication System

Adams W. K. Kong, *Member, IEEE,*
David Zhang, *Senior Member, IEEE,*
and Mohamed Kamel, *Fellow, IEEE*

***Abstract*—Biometric authentication systems are widely applied because they offer inherent advantages over classical knowledge-based and token-based personal-identification approaches. This has led to the development of products using palmprints as biometric traits and their use in several real applications. However, as biometric systems are vulnerable to replay, database, and brute-force attacks, such potential attacks must be analyzed before biometric systems are massively deployed in security systems. This correspondence proposes a projected multinomial distribution for studying the probability of successfully using brute-force attacks to break into a palmprint system. To validate the proposed model, we have conducted a simulation. Its results demonstrate that the proposed model can accurately estimate the probability. The proposed model indicates that it is computationally infeasible to break into the palmprint system using brute-force attacks.**

***Index Terms*—Brute-force attack, palmprint, passwords, secure authentication.**

I. Introduction

Current security systems that automatically identify individuals commonly use either tokens of private knowledge such as a password or a private possession such as a smart card. Such tokens are insecure in that they can be lost, shared, stolen, or duplicated. In this respect, biometric authentication approaches that use physiological and behavioral characteristics such as the iris, retina, fingerprint, palmprint, signature, or gait [2] are much more secure. They are not, however, invulnerable. For example, they are open to database, replay, and brute-force attacks.

Fig. 1 shows a number of points, Points 1–8, all being vulnerable points as identified by the studies in [4] and [5]. The potential attack points are between and on the common components of a biometric system, input sensor, feature extractor, matcher, and database, and are especially open to attack when the biometric systems are employed on remote and unattended applications, giving the attackers enough time to make complex and numerous attempts to break in. At Point 1, a system can be spoofed using fake biometrics such as artificial gummy fingerprints and face masks [6]. At Point 2, it is possible to avoid liveness tests in the sensors by using a prerecorded biometric signal such as a fingerprint image. This is a so-called replay attack. At Point 3, the original output features can be replaced with a predefined feature by using a Trojan horse to override the feature-extraction process. At Point 4, it is possible to use both the brute-force and replay attacks, submitting on the one hand numerous synthetic templates or, on the other, prerecorded templates. At Point 5, original matching scores can be replaced with preselected matching scores by using a Trojan horse. At Point 6, it is possible to insert templates from unauthorized users into the database or to modify templates in the database. At Point 7, replay attacks are once again possible. At Point 8, it is possible to override the system's decision output and to collect the matching scores to generate the images in the registered database [15].

Recently, many biometric and security researchers have proposed techniques for preventing and detecting these attacks [3]–[5], [7]–[9], [12], [17], [22], [23]. Some researchers have employed watermarking and encryption to prevent replay attacks at Points 2, 4, and 7 [9], [17], [22] and have developed antispoofing techniques for specific biometrics to prevent attacks at Point 1 [3], [12]. Other researchers have produced analyses of specific attack types vis-à-vis specific biometrics, for example, the brute-force attacks at Point 4 of the fingerprint systems [4], [5], [7]. Unfortunately, the analysis of the brute-force break-ins against the fingerprint systems is not applicable to the palmprint systems since the template formats of the fingerprints and the palmprints are different.

Given the commercial potential of the palmprint systems as security applications, the wide variety of capture devices that now exist, and the diversity of preprocessing, feature-extraction, matching, and classification algorithms [1], [10], [11], [16], [18]–[20] that have been produced in the field over the last seven years, it is certainly the case that any security issues should be systematically addressed prior to their widespread deployment. In this correspondence, we respond to this need by being the first, to our knowledge, to successfully consider security issues in the palmprint systems. Initially, we concentrate on the brute-force attacks at Point 4. We will discuss other potential attacks in forthcoming papers.

To prevent the brute-force attacks, the security systems based on passwords allow a limited number of traits within a period of time. The systems block the access for a certain amount of period if the limit is over. However, this scheme is not suitable for identification systems (one-to-many matching systems), as the palmprint system described in this correspondence, since this scheme would block the accesses of all users.

The rest of this correspondence is organized as follows. Section II provides a brief summary of our palmprint system. Section III develops a probabilistic model describing the relationship between false-acceptance rates and the number of attacks. Section IV validates the proposed model and gives the experimental results. Section V offers some concluding remarks.

II. Summary of the Palmprint System Exploiting Competitive Code

In this section, we briefly introduce our system, which employs a palmprint-identification algorithm known as Competitive Code [19]. We choose to analyze Competitive Code in the context of brute-force attacks rather than other palmprint-verification algorithms [13], [14], [21] because it is the most accurate and the computationally fastest algorithm developed by Zhang and his coworkers. The version of Competitive Code used in this correspondence has been modified so that it can reissue new templates when original templates have been compromised. In other words, the new Competitive Code provides a cancelable palmprint representation [4], [5], [7].

Manuscript received June 30, 2005; revised November 16, 2005 and March 15, 2006. This paper was recommended by Associate Editor Q. Zhu.

A. W. K. Kong is with the Pattern Analysis and Machine Intelligence (PAMI) Group, Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada and also with the Biometric Research Centre, The Hong Kong Polytechnic University, Hung Hom, Hong Kong (e-mail: adamskong@ieee.org).

D. Zhang is with the Biometric Research Centre, Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong (e-mail: csdzhang@comp.polyu.edu.hk).

M. Kamel is with the PAMI Group, Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: mkamel@uwaterloo.ca).

Digital Object Identifier 10.1109/TSMCB.2006.876168

1083-4419/$20.00 © 2006 IEEE

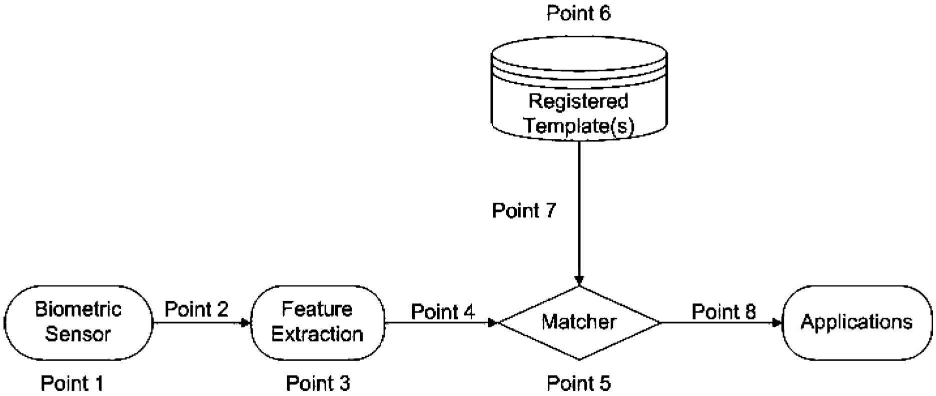

Fig. 1. Potential attack points in a biometric system.

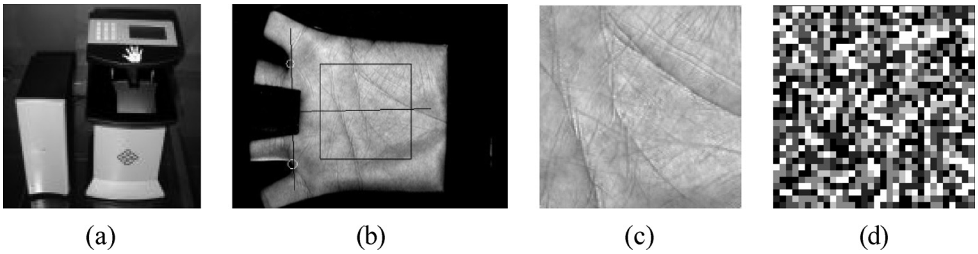

Fig. 2. Palmprint-identification system using Competitive Code. (a) Palmprint scanner developed by the Biometrics Research Centre, The Hong Kong Polytechnic University, (b) key points and coordinate system for palmprint segmentation and alignment, (c) preprocessed palmprint image for feature extraction, and (d) Competitive Code, where different colors represent different orientations.

Like other biometric systems, a typical palmprint verification or identification system consists of four components: an image-acquisition component, a preprocessing component, a feature-extraction component, and a matching component [10], [11], [16]. The specifics of the four components of our system are as follows.

1) *Image acquirer:* This component transmits a palmprint image from the palmprint scanner to a computer. Fig. 2(a) shows a palmprint scanner developed by the Biometrics Research Centre of The Hong Kong Polytechnic University. Its design principles can be found in [10].
2) *Preprocessor:* This component detects the two key points between fingers to establish a coordinate system for aligning the different palmprint images. The coordinate system is then used to extract the central parts of the palmprint images. Fig. 2(b) shows the key points and the coordinate system, and Fig. 2(c) shows a preprocessed palmprint image.
3) *Feature extractor:* Our original algorithm applies six real Gabor filters with fixed orientations to a preprocessed palmprint image, $I(x,y)$ [19] to estimate the local orientation field as features. The filters are defined as

$$\psi(x,y,x_0,y_0,\omega,\theta,\kappa) = \frac{\omega}{\sqrt{2\pi}\kappa} e^{-\frac{\omega^2}{8\kappa^2}(4x'^2+y'^2)} \times \left(\cos(\omega x') - e^{-\frac{\kappa^2}{2}}\right) \quad (1)$$

where $x' = (x-x_0)\cos\theta + (y-y_0)\sin\theta$, $y' = -(x-x_0)\sin\theta + (y-y_0)\cos\theta$, (x_0,y_0) is the center of the function, ω is the radial frequency in radians per unit length, and θ is the orientation of the Gabor filters in radians. κ is defined as $\kappa = \sqrt{2\ln 2}((2^\delta+1)/(2^\delta-1))$, where δ is the half-amplitude bandwidth of the frequency response. The original orientations of the six filters, θ_v are $v\pi/6$, where $v = 0,1,2,3,4,$ and 5. The orientation of a local region is estimated using a competitive rule, $k = \arg(\min_v(I(x,y)^*\psi(x,y,x_0,y_0,\omega,\theta_v,\kappa))$ where $*$ represents convolution and k is called the winning index. To achieve a cancelable representation, we embed a random field $\alpha(x_0,y_0)$ following a uniform distribution with support 0, $\pi/6$, $2\pi/6$, $3\pi/6$, $4\pi/6$, and $5\pi/6$. The value of $\alpha(x_0,y_0)$ depends on the filter center (x_0,y_0). As the result, the competitive rule becomes $k = \arg(\min_v(I(x,y)^*\psi(x,y,x_0,y_0,\omega,\theta_v + \alpha(x_0,y_0),\kappa))$. When we reissue a new template, we need only to replace the original random field with a new random field. Fig. 2(d) shows a final feature code. The random field destroys all the line features and therefore looks like a noisy image. We still refer to the final feature code as Competitive Code.
4) *Angular comparer:* This component compares two Competitive Codes by using an angular distance. Table I gives all the possible angular distances between two winning indexes. Summing up all the angular distances at different positions, we have the angular distance between two Competitive Codes defined as

$$A_f(P,Q) = \sum_{x=1}^{32}\sum_{y=1}^{32} A(P_{x,y},Q_{x,y}) \quad (2)$$

where $P_{x,y}(Q_{x,y})$ is a winning index of Competitive Code, $P(Q)$ at position (x,y) and $A(P_{x,y},Q_{x,y})$ is the angular distance between the two winning indexes. To support a real-time identification in large databases, we provide a coding scheme to encode the winning indexes so that we can implement angular distance using Boolean operators. Table II gives the coding scheme. The corresponding bitwise angular distance is defined as

$$A_f(P,Q) = \sum_{x=1}^{32}\sum_{y=1}^{32}\sum_{i=1}^{3} P_i^b(x,y) \otimes Q_i^b(x,y) \quad (3)$$

TABLE I
ALL POSSIBLE ANGULAR DISTANCES BETWEEN DIFFERENT WINNING INDEXES

Angular Distance		Winning indexes, $P_{x,y}$					
$A(P_{x,y}, Q_{x,y})$		0	1	2	3	4	5
Winning indexes $Q_{x,y}$	0	0	1	2	3	2	1
	1	1	0	1	2	3	2
	2	2	1	0	1	2	3
	3	3	2	1	0	1	2
	4	2	3	2	1	0	1
	5	1	2	3	2	1	0

TABLE II
BITWISE REPRESENTATION OF COMPETITIVE CODE

Winning indexes	Bit 1	Bit 2	Bit 3
0	0	0	0
1	0	0	1
2	0	1	1
3	1	1	1
4	1	1	0
5	1	0	0

where $P_i^b(Q_i^b)$ is the ith bit plane of $P(Q)$ and $\otimes$ is the bitwise exclusive OR. Occasionally, as a result of the incorrect placement of hands, some palmprints contain nonpalmprint pixels. All the nonpalmprint pixels are black since they belong to the capture device. We can use a simple threshold to classify them. We use a bit plane as a mask to denote the nonpalmprint pixels. Finally, the bitwise angular distance is defined as

$$A_f(P,Q) = \frac{\sum_{y=1}^{32}\sum_{x=1}^{32}\sum_{i=1}^{3}\left(P_M(x,y)\cap Q_M(x,y)\right)\cap\left(P_i^b(x,y)\otimes Q_i^b(x,y)\right)}{3\sum_{y=1}^{32}\sum_{x=1}^{32}P_M(x,y)\cap Q_M(x,y)} \tag{4}$$

where $\cap$ is the bitwise AND and $P_M(Q_M)$ is the mask of $P(Q)$. Obviously, A_f is between 0 and 1. For a perfect matching, the angular distance is zero. To account for alignment imperfections, we generate 25 translated Competitive Codes by translating the preprocessed image. In other words, we have 25 angular distances when we match two palmprints. The minimum of these distances is regarded as the final angular distance, A_F. Using a 3-GHz processor, the bitwise angular distance can make 100 000 comparisons/s.

III. PROBABILISTIC MODEL FOR ANALYZING BRUTE-FORCE BREAK-INS

The study of the brute-force break-ins requires a probabilistic model that describes the relationship between the number of attacks and the probability of a false acceptance. Therefore, it is necessary to establish a probabilistic model for the angular distance given in (4). To simplify the model, we assume that all the preprocessed palmprint images are clear and devoid of the nonpalmprint pixels. This will allow us to neglect the masks and the normalization terms. We could get exactly the same result for this analysis by using either the integer representation or the bitwise representation of Competitive Code, but for the purposes of the presentation, it is more convenient to use the integer representation. Thus, we consider the angular distance given in (2) for the following analysis.

TABLE III
DISTRIBUTION OF WINNING INDEXES

Winning index	0	1	2	3	4	5
Probability	0.166	0.167	0.168	0.166	0.166	0.167

Let $W = [w_0, w_1, w_2, w_3]$ be a random vector where w_i is the number of $A(P_{x,y}, Q_{x,y}) = i$ in (2), and let p_i be the probability of $A(P_{x,y}, Q_{x,y}) = i$. As a result, the angular distance described in (2) can be rewritten as $A_f(P,Q) = WK^T$, where $K = [0, 1, 2, 3]$. We assume that p_i is stationary and $A(P_{x,y}, Q_{x,y})$ is independent. By stationary, we mean that p_i does not depend on the position (x, y). Using these assumptions, we infer that W follows multinomial distribution, i.e.,

$$f(w_0, w_1, w_2, w_3) = \frac{n!}{w_0!w_1!w_2!w_3!}p_0^{w_0}p_1^{w_1}p_2^{w_2}p_3^{w_3} \tag{5}$$

where n is equal to 1024, the size of the Competitive Codes. Thus, the probability density function of the angular distance $A_f(P,Q)$ is

$$\Pr\left(A_f(P,Q) = t\right) = \sum_{W \ni WK^T = t} f(w_o, w_1, w_2, w_3). \tag{6}$$

Since f is a multinomial distribution and the summation can be regarded as a projection on the line $WK^T = t$, we call this distribution "projected multinomial distribution."

Let $\Pr(A_f(P,Q) < t) = F(t)$ and therefore $\Pr(A_f(P,Q) \geq t) = 1 - F(t)$, where $F(t)$ is the cumulative distribution of $A_f(P,Q)$. The probability of the final angular distance A_F being greater than the threshold t is

$$\Pr\left(A_F(P,Q) \geq t\right) = \left(1 - F(t)\right)^m \tag{7}$$

where m, the number of translated matchings, is 25. If we make z independent comparisons, the probability of all the final angular distances being greater than or equal to t is

$$\Pr\left(A_F(P_i,Q_i) \geq t | \forall i = 1, \ldots, z\right) = \left(1 - F(t)\right)^{mz} \tag{8}$$

where P_i and Q_i represent the different Competitive Codes. Consequently, the probability of at least one of the final angular distances being shorter than t is

$$\Pr\left(\min_i\left(A_F(P_i,Q_i)\right) < t\right) = 1 - \left(1 - F(t)\right)^{mz}. \tag{9}$$

We can now analyze the brute-force attacks against our palmprint system using (9). For verification, each attackers' template, P_i is compared only with the templates associated with a particular user.

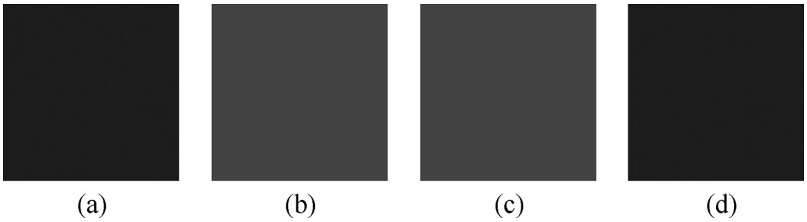

Fig. 3. (a)–(d) Estimated $p_0 p_3$ at different positions, respectively, where black represents probability zero while white represents probability one.

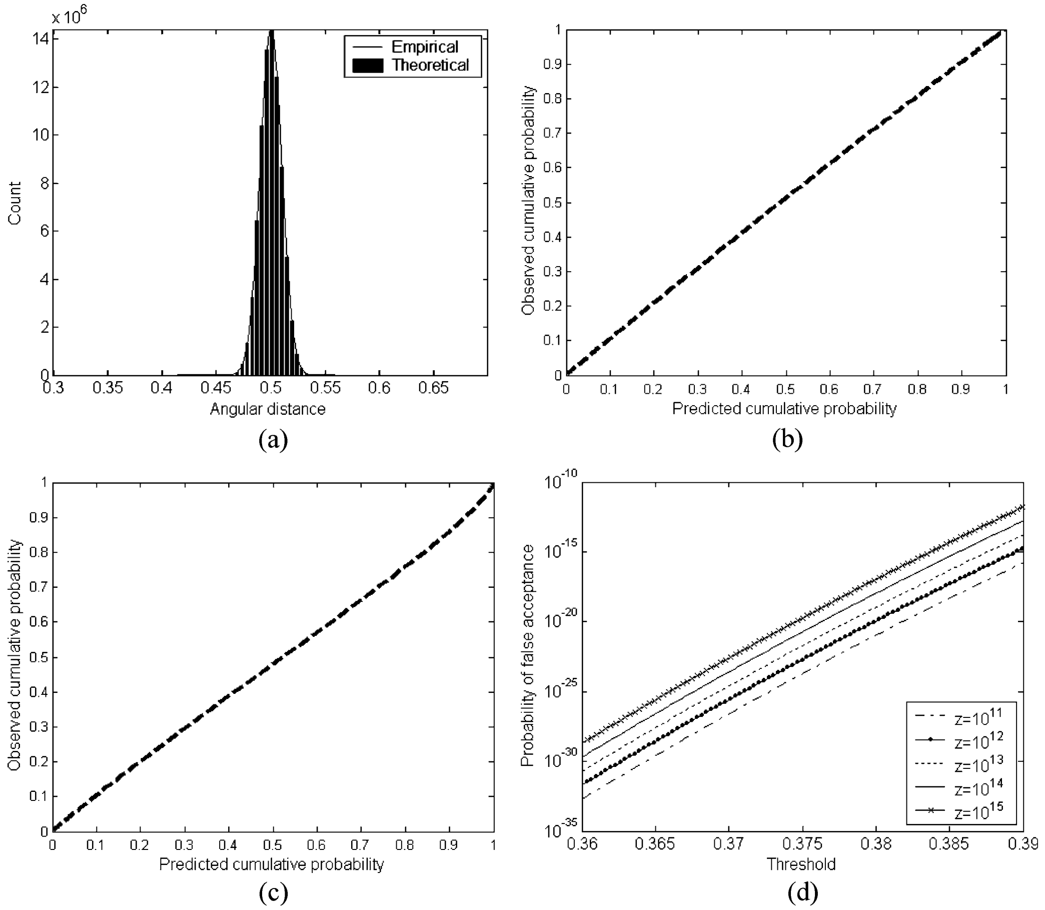

Fig. 4. Model validation and predications. (a) Empirical and theoretical distributions from nontranslated matchings, (b) plot of predicted cumulative probability against the observed cumulative probability for nontranslated matchings, (c) plot of the predicted cumulative probability against the observed cumulative probability for translated matching, and (d) probability of the false acceptances against different thresholds.

We assume that each user only has one template Q in the database, and to attack the system the hackers submit z templates. The probability of a false acceptance for verification is

$$\Pr\left(\min_i A_F(P_i, Q) < t\right) = 1 - (1 - F(t))^{mz} \qquad (10)$$

the same as in (9).

For identification, each submitted template P_i as a brute-force attack is compared with all the templates in the database. Let the templates in the database be Q_j where $j = 1, \ldots, b$. As in the previous discussion, we let the number of the templates for the brute-force attack be z. Therefore, the probability of the false acceptance occurring in an identification system with b templates in the database is

$$\Pr\left(\min_{i,j} A_F(P_i, Q_j) < t\right) = 1 - (1 - F(t))^{mzb}. \qquad (11)$$

Equation (10) for verification and (11) for identification each share the same form. Thus, for simplicity of the presentation, we shall consider only verification in the following experiments.

IV. Model Validation and Experimental Results

The use of the probabilistic model to analyze the brute-force attacks requires us to make some assumptions when obtaining the model parameters p_i. We assume that the winning indexes of Competitive Code Q follow independent uniform distributions. In other words, $\Pr(Q_{x,y} = v) = 1/6$, for all $v = 0, 1, 2, 3, 4,$ and 5. This assumption holds since the random field is formed by the independent uniform distributions. We do not make any assumptions as to the winning indexes of the artificial Competitive Codes P_i. Let c_v be the probability of the winning index of P_i being equal to v. Using Table I, we can infer that $p_0 = \sum_{v=0}^{5} c_v/6 = 1/6$, $p_1 = 2\sum_{v=0}^{5} c_v/6 = 1/3$, $p_2 = 2\sum_{v=0}^{5} c_v/6 = 1/3$, and $p_3 = \sum_{v=0}^{5} c_v/6 = 1/6$.

Now that we have all the model parameters, we run a simulation to validate the proposed model. For this simulation, we collect 11 074 palmprint images from 568 different palms. The images are 384 × 284, and they have a resolution of 75 dpi. First of all, we use 100 different random fields to compute the Competitive Codes. Then, we use uniform distribution to generate 100 artificial Competitive Codes to attack each Competitive Code. Each artificial Competitive Code is matched with the true Competitive Code as a brute-force attack. Using the true Competitive Codes, we estimate the distribution of the winning indexes in Table III, demonstrating that the winning index follows a uniform distribution. We also estimate p_0, p_1, p_2, and p_3 at different positions in Fig. 3, where black represents a probability zero while white represents a probability one. Fig. 3 demonstrates that the stationary assumption for p_i is held. The empirical distribution and the proposed theoretical distribution of nontranslated matchings are given in Fig. 4(a). We also plot the predicted cumulative probability against the observed cumulative probability from the nontranslated matchings and translated matchings in Fig. 4(b) and (c), respectively. Fig. 4(a)–(c) demonstrates the predictive power of the proposed model.

Now, we can use the proposed model to estimate the probability of the successful break-ins. Fig. 4(d) plots the probability of the false acceptance against different thresholds. We show only the threshold between 0.36 and 0.39 since our system generally operates in this range. Assume that our system can make one million comparisons, ten times faster than our current implementations. The corresponding computation times for $z = 10^{11}, 10^{12}, 10^{13}, 10^{14},$ and 10^{15} are 1.16 days, 11.5 days, 115 days, 3.17 years, and 31.7 years, respectively. The computation times and the probabilities of the false acceptances demonstrate that it is impossible to use brute force to break into our system.

V. Conclusion

This correspondence presents a systematic analysis of the brute-force break-ins directed against our palmprint system. Using Competitive Code as the features and angular distance as the matching scheme, we set up a projected multinomial distribution to describe the relationship between the probability of the false acceptance and the number of attacks. According to our analysis, when the system threshold is set to lower than 0.39, it is computationally infeasible to break into our palmprint system using brute-force attacks.

Acknowledgment

The authors would like to thank the reviewers for their valuable comments.

References

[1] W. Shu and D. Zhang, "Automated personal identification by palmprint," *Opt. Eng.*, vol. 37, no. 8, pp. 2359–2363, Aug. 1998.

[2] A. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*, Boston, MA: Kluwer, 1999.

[3] J. Daugman, "Recognizing persons by their iris patterns," in *Biometrics: Personal Identification in Networked Society*. Amsterdam, The Netherlands: Kluwer, 1999, pp. 103–121.

[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Aug. 2001.

[5] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognit.*, vol. 35, no. 12, pp. 2727–2738, Dec. 2002.

[6] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," *Proc. SPIE*, vol. 4677, pp. 275–289, Feb 2002.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Biometrics break-ins and band-aids," *Pattern Recognit. Lett.*, vol. 24, no. 13, pp. 2105–2113, Sep. 2003.

[8] L. O'Gorman, "Comparing passwords, tokens, biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[9] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[10] D. Zhang, W. K. Kong, J. You, and M. Wong, "On-line palmprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1041–1050, Sep. 2003.

[11] C. C. Han, H. L. Cheng, K. C. Fan, and C. L. Lin, "Personal authentication using palmprint features," *Pattern Recognit.*, vol. 36, no. 2, pp. 371–381, Feb. 2003.

[12] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recognit.*, vol. 36, no. 2, pp. 383–396, Feb. 2003.

[13] G. Lu, D. Zhang, and K. Wang, "Palmprint recognition using eigenpalms features," *Pattern Recognit. Lett.*, vol. 24, no. 9, pp. 1463–1467, 2003.

[14] X. Wu, D. Zhang, and K. Wang, "Fisherpalms based palmprint recognition," *Pattern Recognit. Lett.*, vol. 24, no. 15, pp. 2829–2838, Nov. 2003.

[15] A. Adler, "Sample images can be independently restored from face recognition templates," in *Proc. Can. Conf. Elect. and Comput. Eng.*, Montreal, QC, Canada, 2003, pp. 1163–1166.

[16] C. C. Han, "A hand-based personal authentication using a coarse-to-fine strategy," *Image Vis. Comput.*, vol. 22, no. 11, pp. 909–918, Sep. 2004.

[17] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[18] X. Wu, D. Zhang, K. Wang, and B. Hung, "Palmprint classification using principal lines," *Pattern Recognit.*, vol. 37, no. 10, pp. 1987–1998, Oct. 2004.

[19] A. W. K. Kong and D. Zhang, "Competitive coding scheme for palmprint verification," in *Proc. Int. Conf. Pattern Recognit.*, 2004, vol. 1, pp. 520–523.

[20] Y. H. Pang, A. T. B. Toeh, D. C. L. Ngo, and H. F. San, "Palmprint verification with moments," *J. Comput. Graph. Vis. Comput. Vis.*, vol. 12, no. 2, pp. 325–332, 2004.

[21] L. Zhang and D. Zhang, "Characterization of palmprints by wavelet signatures via directional context modeling," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 34, no. 3, pp. 1335–1347, Jun. 2004.

[22] M. Vatsa, R. Singh, P. Mitra, and A. Noore, "Comparing robustness of watermarking algorithms on biometric data," in *Proc. Workshop Biometric Challenges from Theory Practice*, 2004, pp. 5–8.

[23] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," in *Proc. SPIE-EI—Security, Seganography and Watermarking Multimedia Contents VI*, 2004, pp. 622–633.