A Study of Brute-Force Break-ins of a Palmprint Verification System

Adams Kong[1,2], David Zhang[1] and Mohamed Kamel[2]

[1] Biometrics Research Centre, Department of Computing,
Hong Kong Polytechnic University, Kowloon, Hong Kong
adamskong@ieee.org
csdzhang@comp.polyu.edu.hk
[2] Pattern Analysis and Machine Intelligence Lab,
University of Waterloo, 200 University Avenue West, Ontario, Canada
mkamel@uwaterloo.ca

Abstract. Biometric systems are widely applied since they offer inherent advantages over traditional knowledge-based and token-based personal authentication approaches. This has led to the development of palmprint systems and their use in several real applications. Biometric systems are not, however, invulnerable. The potential attacks including replay and brute-force attacks have to be analyzed before they are massively deployed in real applications. With this in mind, this paper will consider brute-force break-ins directed against palmprint verification systems.

1 Introduction

Accurate automatic personal authentication does not only act as an important means for protecting our lives and properties, it is also an integral element in the ever rapidly expanding e-applications arena, playing in our everyday encounters such as e-banking, e-commerce, e-kiosks, etc. Traditional security systems which automatically identify individuals generally use either tokens of private possessions such as a physical key or private knowledge such as a password. Such tokens are insecure. They can be shared, duplicated, lost or stolen. In this respect, biometric systems that recognize individuals based on their physiological and behavioral characteristics such as the fingerprint, face, iris, palmprint or signature are much more secure. However, they are not invulnerable. For instance, the systems can be broken into using replay and brute-force attacks.

Fig. 1 shows a generic biometric system, where Points 1-8 are vulnerable points as identified by [2-3]. At Point 1, a system is able to be spoofed using fake biometrics e.g. face masks and artificial gummy fingerprints [4]. At Point 2, liveness detection countermeasures in the sensors can be avoided by using a pre-recorded signal such as iris image. This is a so-called replay attack. At Point 3, a Trojan horse can override the feature extraction process so that the original output features are replaced with a predefined feature. At Point 4, it is possible to use both replay and brute-force attacks,

註解: added e-kiosks here to make the punctuation and flow of article right, please feel free to delete this.

submitting on the one hand prerecorded templates or, on the other, numerous synthetic templates. At Point 5, the matching scores obtained can be replaced with preselected matching scores by using a Trojan horse. At Point 6, it is possible to modify templates in the database or to insert templates from unauthorized users into the database. At Point 7, replay attacks are once again possible. At Point 8, it is possible to directly override the decision output of the system.

In remote, unattended applications, such as web-based e-commerce applications, attackers may have enough time to make complex and numerous attempts to break in. Security and biometric researchers have recently proposed methods for detecting and preventing these attacks [2-3, 5-8]. Some researchers have analyzed specific attack types vis-à-vis specific biometrics, for instance, brute-force attacks at Point 4 of fingerprint systems [2-3, 5].

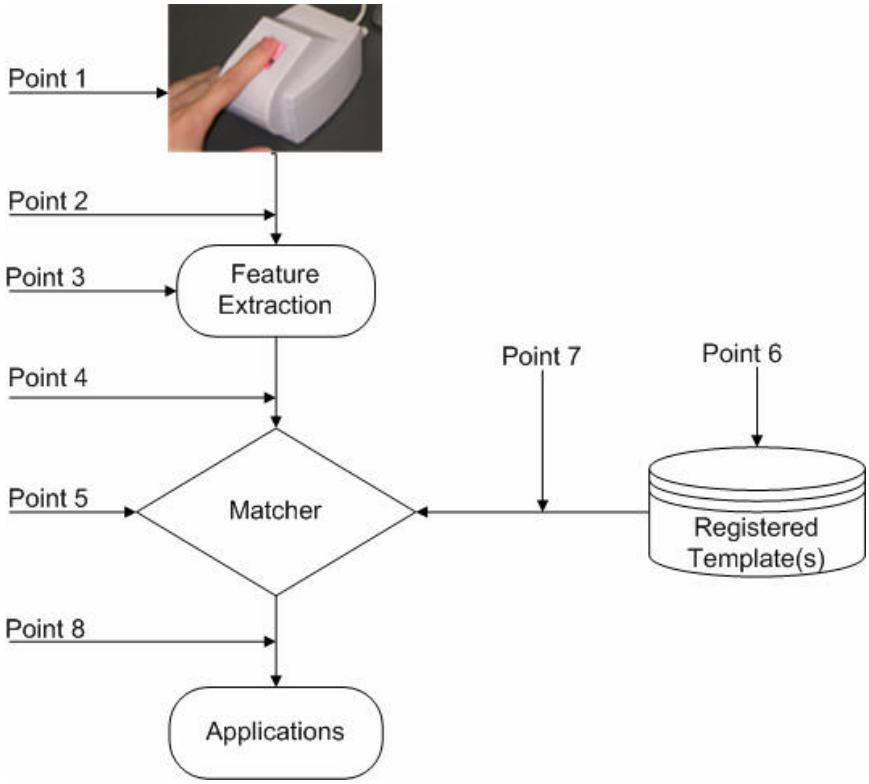

Fig. 1. Vulnerable points in a biometric system

Given the commercial potential of palmprint systems and the variety of capture devices, and preprocessing, feature extraction, matching and classification algorithms [9-16] that have been developed over the last several years, it is certainly the case that any security issues should be systematically addressed prior to their widespread deployment. In this paper, we concentrate on brute-force attacks at Point 4. As far as we know, this is the first paper that considers security issues in palmprint systems.

The rest of this paper is organized as the follows. Section 2 gives an overview of the palmprint system for this analysis. Section 3 provides a probabilistic model describing the relationship between number of attacks and false acceptance rates. Section 4 provides experimental results. Finally, Section 5 offers some concluding remarks and further research directions.

2 A Summary of the Palmprint System Using Competitive Code

In this Section, we introduce our palmprint system using a palmprint identification algorithm known as Competitive Code [13-14]. We select to study Competitive Code in the context of brute-force attacks rather than other palmprint algorithms since it is the most accurate and fastest algorithm developed by us [10, 15, 17-19]. Precisely, Competitive Code can operate at a high genuine acceptance rate of 98.4% while the corresponding false acceptance rate is 3×10^{-6}% [14]. The computation speed of Competitive Code can be comparable with IrisCode [20] since the angular distance is implemented using Boolean operators. In addition to speed and accuracy, Competitive Code can effectively distinguish the palmprints of identical twins [16]. Our system using Competitive Code consists of the following parts.

Image acquisition: Transmit a palmprint image to a processor from a palmprint scanner [13]. Fig. 2(a) shows a palmprint scanner developed by the Biometrics Research Centre, The Hong Kong Polytechnic University and Fig. 2(b) shows a collected palmprint image.

Preprocessing: Determine the two key points between fingers to establish a coordinate system for aligning different palmprint images [13]. Then, extract the central parts on the base of the coordinate system. Fig. 2(c) illustrates the key points and the coordinate system and Fig. 2(d) shows a preprocessed palmprint image.

Feature extraction: The real parts of six Gabor filters with different orientations, $y_R(x, y, q_j)$, where q_j represents the orientation of the filters are applied to a preprocessed palmprint image, *I(x,y)* [14]. The orientation of a sample point is estimated using a competitive rule, $k=arg(min_j(I(x,y)*y_R(x,y,?_j)))$, where *k* is called the winning index and *j=0, 1, 2, 3, 4,* and *5*. Combining the winning indexes at different sample points, we have the final feature, called Competitive Code.

Coding: For effective matching, the winning indexes are coded using Table 1. Three bits are used to represent one winning index.

Angular comparison: The difference between two Competitive Codes is measured using their angular distance. The bitwise representation of angular distance is defined as:

$$A_H(P,Q) = \frac{\sum_{y=1}^{N}\sum_{x=1}^{N}\sum_{i=1}^{3}(P_M(x,y) \cap Q_M(x,y)) \cap (P_i^b(x,y) \otimes Q_i^b(x,y))}{3\sum_{y=1}^{N}\sum_{x=1}^{N} P_M(x,y) \cap Q_M(x,y)} \quad (1)$$

where $P_i^b\left(Q_i^b\right)$ is the i^{th} bit plane of Competitive Code *P(Q)*; $P_M(Q_M)$ is the mask of *P(Q)* used to denote the non-palmprint pixels; $\otimes$ is bitwise exclusive OR; $\cap$ is bitwise AND and N^2 is the size of Competitive Code. Obviously, A_H is between 0 and 1. Since the preprocessing algorithm is not perfect, one of the features must be translated horizontally and vertically and then the matching is carried out again. The ranges of both the horizontal and the vertical translations are –2 to 2.The minimum of the A_H's obtained by translated matching is regarded as the final angular distance, A_f .

Table 1. Bitwise representation of the Competitive Code

Winning index	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

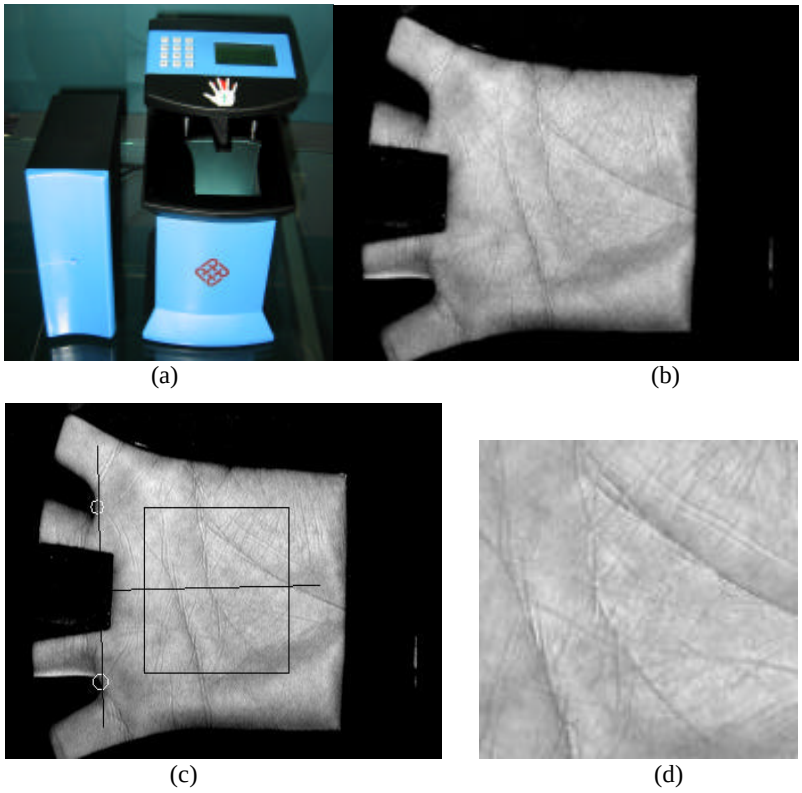

Fig. 2. Illustration of palmprint collection and pre-processing: a) a palmprint scanner developed by the Biometrics Research Centre, The Hong Kong Polytechnic University, b) a collected palmprint image, c) the key points and coordinate system for palmprint segmentation and alignment and d) the pre-processed palmprint image for the proposed framework.

3 A Probabilistic Model for Studying Brute-Force Break-ins

To analyze brute-force break-ins, we have to develop a probabilistic model that describes the relationship between the probability of a false acceptance and the numbers of attacks. In other words, we require a probabilistic model for the angular distance described in Eq. 1. To simplify the model, we assume that all preprocessed palmprint images contain no non-palmprint pixels. This will allow us to neglect the normalization constant and the masks. For the sake of convenience, we employ the integer representation of Competitive Code rather than the bitwise representation for the following analysis. As a result, the angular distance between two Competitive Codes is

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

where $A(P_{x,y}, Q_{x,y})$ is the angular distance between two winning indexes, $P_{x,y}$ and $Q_{x,y}$. Table 2 gives all possible angular distances.

Let $W = [w_o, w_1, w_2, w_3]$ be a random vector where w_i is the number of $A(P_{x,y}, Q_{x,y}) = i$ in Eq. 2 and let p_i be the probability of $A(P_{x,y}, Q_{x,y}) = i$. Consequently, we can rewrite the angular distance described in Eq. 2 as $A_H(P,Q) = WK^T$, where $K = [0, 1, 2, 3]$. We also assume that $A(P_{x,y}, Q_{x,y})$ is independent and p_i is stationary. By "stationary" we mean that p_i does not depend on the position *(x, y)*. Similar assumptions have been employed in analyzing brute-force break-ins of fingerprint systems [2-3]. Using these assumptions, we can infer that *W* follows multinomial distribution i.e.

$$f(w_0, w_1, w_2, w_3) = \frac{n!}{w_0!\, w_1!\, w_2!\, w_3!}\, p_0^{w_0}\, p_1^{w_1}\, p_2^{w_2}\, p_3^{w_3}, \quad (3)$$

where *n* is equal to N^2, the effective matching area. Therefore, the probability density of the angular distance is,

$$\Pr(A_H(P,Q) = t) = \sum_{W \ni WK^T = t} f(w_o, w_1, w_2, w_3). \quad (4)$$

So far, we have established a probability model in which the model parameter *n* depends on the effective matching area. This area changes according to the translated matchings. To simplify the following formulation, we treat all the translated matchings as having the same effective matching area, i.e., 900. It is the minimum matching area.

Let $\Pr(A_H(P,Q) < t) = F(t)$ and thus, $\Pr(A_H(P,Q) \geq t) = 1 - F(t)$. The probability of the final angular distance A_f being greater than the threshold *t* is

$$\Pr(A_f(P,Q) \geq t) = (1 - F(t))^m, \quad (5)$$

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

$$\Pr(A_f(P_i, Q_i) \geq t \mid \forall i = 1,..., z) = (1 - F(t))^{mz}, \quad (6)$$

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

$$\Pr(A_f(P_i, Q_i) < t) = 1 - (1 - F(t))^{mz}. \quad (7)$$

Now, we are able to analyze brute-force attacks against our system using Eq. 7. For verification, each submitted templates, P_i as a brute-force attack, is matched with the templates associated with a particular user. We assume that each user only has one template, Q in the database and the hackers submit z templates to attack the system. Therefore, the probability of a false acceptance for verification is

$$\Pr(A_f(P_i, Q) < t) = 1 - (1 - F(t))^{mz}, \quad (8)$$

the same as Eq. 7.

Table 2. All possible angular distances between different winning indexes, the elements of Competitive Code

Angular distance		Winning indexes					
		0	1	2	3	4	5
Winning indexes	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

4 Parameter Estimation and Experimental Results

The use of the probabilistic model to investigate brute-force break-ins into our palmprint system requires us to make some assumptions to obtain the model parameters, p_i. We suppose that the attackers use uniform distributions to generate the winning indexes of their synthetic Competitive Codes. We also assume that the winning indexes of the template, Q, in database follow uniform distribution and all of their winning indexes are independent, we can infer that

$$p_0 = p_3 = 1/6 \quad (9)$$

and

$$p_1 = p_2 = 1/3 \quad (10)$$

from Table 2. Using these parameters and Eq. 7, we can estimate the probability of false acceptance at different thresholds and under different number attacks, z. Fig. 3 shows the experimental results but only provides the thresholds in the range between

0.34 and 0.4 since they associate with acceptable false acceptance (general case, not brute-force attack) and false rejection rates for our palmprint system. Our system generally operates at the threshold 0.37, at which threshold, it has a false acceptance rate of 0×10^{-6}% and a genuine acceptance rate of 97.7% [14]. Table 3 lists the probabilities of a false acceptance of brute-force attacks and the corresponding computation time when the threshold is set to 0.37. We assume that the system can make 1 million comparisons per second to estimate the computation time. Fig. 3 and Table 3 show that it is computationally infeasible to use a brute-force attack to break in the system.

Table 3. The probabilities of false acceptance under different number attacks, *z* when the threshold is set to 0.37 and the corresponding computation times.

No of attacks z	Time	Probability of false acceptance
10^{11}	1.16 days	9×10^{-24}
10^{12}	11.5 days	9×10^{-23}
10^{13}	115 days	9×10^{-22}
10^{14}	3.17 years	9×10^{-21}
10^{15}	31years	9×10^{-20}

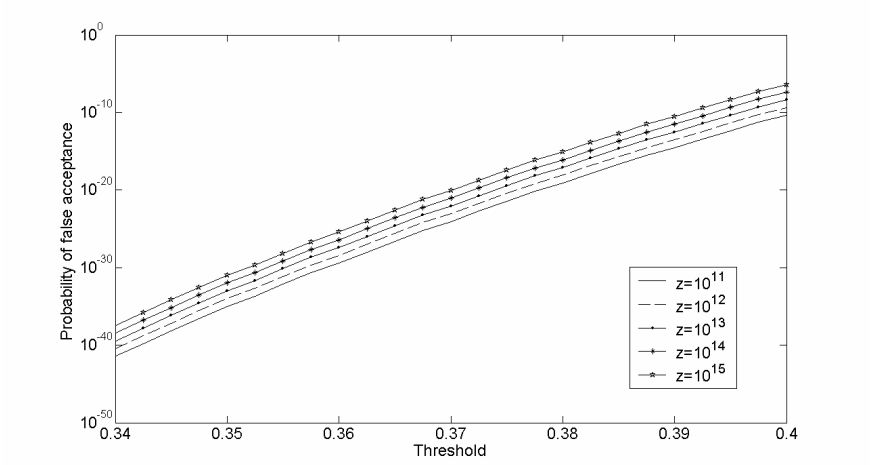

Fig. 3. A plot of the probability of false acceptance against threshold, where *z* represents the number of attacks.

5 Conclusion and Further Research

This paper presents a study of brute-force break-ins directed against our palmprint system that uses Competitive Code as the features and angular distance as the matching scheme. We set up a probabilistic model to describe the relationship between the number of attacks and the probability of false acceptance. According to our analysis, when the system threshold is set to lower than 0.37, it is computationally infeasible to break in our palmprint system using brute-force attacks.

In our previous paper [14], we have developed a bitwise angular distance for matching Competitive Codes. In this paper, we derive a projected multinomial distribution to model the distribution of the angular distance. IrisCode, a well-known biometric recognition method, exploits bitwise hamming distance for comparing two iris features and its imposter distribution is modeled by binomial distribution [20]. The relationships between IrisCode and Competitive Code call for further investigation.

References

1. A. Jain, R. Bolle and S. Pankanti (eds.), *Biometrics: Personal Identification in Networked Society*, Boston, Mass: Kluwer Academic Publishers, 1999.
2. R.M. Bolle, J.H. Connell and N.K. Ratha, "Biometric perils and patches", *Pattern Recognition*, vol. 35, pp. 2727-2738, 2002.
3. N.K. Ratha, J.H. Connell and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001.
4. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems", *Proc, SPIE*, vol. 4677, pp. 275-289, San Jose, USA, Feb, 2002.
5. N.K. Ratha, J.H. Connell and R.M. Bolle, "Biometrics break-ins and band-aids", *Pattern Recognition Letters*, vol. 24, pp, 2105-2113, 2003.
6. L. O'Gorman, "Comparing passwords, tokens, biometrics for user authentication", *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021-2040, 2003.
7. U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, "Biometric cryptosystems: issues and challenges", *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960, 2004.
8. A.K. Jain and U. Uludag, "Hiding biometric data", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494-1498, 2003.
9. W. Shu and D. Zhang, "Automated personal identification by palmprint", *Optical Engineering*, vol. 37, no. 8, pp.2359-2363, 1998.
10. X. Wu, D. Zhang, K. Wang and B. Hung, "Palmprint classification using principal lines", *Pattern recognition*, vol. 37, no. 10, pp. 1987-1998, 2004.
11. C.C. Han, H.L. Cheng, K.C. Fan and C.L. Lin, "Personal authentication using palmprint features", *Pattern Recognition*, vol. 36, no 2, pp. 371-381, 2003.
12. C.C. Han, "A hand-based personal authentication using a coarse-to-fine strategy", *Image and Vision Computing*, vol. 22, pp. 909-918, 2004.
13. D. Zhang, W.K. Kong, J. You and M. Wong, "On-line palmprint identification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041-1050, 2003.

14.A.W.K. Kong and D. Zhang, “Competitive coding scheme for palmprint verification”, *in Proceedings of International Conference on Pattern Recognition*, vol. 1, pp. 520-523, 2004.
15.A.W.K. Kong and D. Zhang, “Feature-level fusion for effective palmprint authentication” *in Proceedings of International Conference on Biometric Authentication*, pp. 761-767, 2004.
16.A. Kong, D Zhang and G. Lu, “A study of identical twins palmprint for personal verification”, *To appear in Pattern Recognition*.
17.W. K. Kong and D. Zhang, “Palmprint texture analysis based on low-resolution images for personal authentication”, *in Proceedings of International Conference on Pattern Recognition*, pp. 807-810, 2002.
18.X. Wu, D. Zhang and K. Wang, “Fisherpalms based palmprint recognition”, *Pattern Recognition Letters*, vol. 24, no. 15, pp. 2829-2838, 2003.
19.L. Zhang and D. Zhang, “Characterization of palmprints by wavelet signatures via directional context modeling”, *IEEE Transactions on Systems, Man and Cybernetics, Part B*, vol. 34, no. 3, pp. 1335-1347, 2004.
20.J. Daugman, “High confidence visual recognition of persons by a test of statistical independence”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-1161, 1993