2009 10th International Conference on Document Analysis and Recognition

Evaluation of Brute-Force Attack to Dynamic Signature Verification Using Synthetic Samples

Javier Galbally, Julian Fierrez, Marcos Martinez-Diaz, and Javier Ortega-Garcia
Biometric Recognition Group–ATVS, EPS, Universidad Autonoma de Madrid
{javier.galbally, julian.fierrez, marcos.matinez, javier.ortega}@uam.es

Abstract

A brute force attack using synthetically generated handwritten signatures is performed against a HMM-based signature recognition system. The generation algorithm of synthetic signatures is based on the spectral analysis of the trajectory functions and has proven to produce very realistic results. The experiments are carried out by attacking real signature models from the MCYT database (which comprises 8,250 signature samples from 330 users). Results show that such an attack is feasible, thus arising the necessity of introducing countermeasures against this type of vulnerability in real applications.

1 Introduction

Due to the advantages that biometric security systems present over traditional security approaches [9], they are currently being introduced in many applications, including: access control, sensitive data protection, on-line tracking systems, etc. However, in spite of these advantages they are not free from external attacks which can decrease their level of security. Thus, it is of utmost importance to analyze the vulnerabilities of biometric systems [6, 8, 14], in order to find their limitations and to develop useful countermeasures for foreseeable attacks.

From all the possible vulnerability threats that biometric systems might present, one of them, which arises from their inherent probabilistic nature, is common to all automatic recognition systems: there is always a certain probability of accessing the system with a different biometric trait to that of the genuine user. This probability, which is represented by the False Acceptance Rate (FAR) at each operating point, is the origin of the so called brute force attacks [11]. This type of attacks try to take advantage of this security breach by presenting to the system successive biometric samples until one of them obtains a positive answer from the system.

Apart from possible countermeasures that could be included in recognition systems, such as limiting the number of consecutive access attempts, the main drawback of brute force attacks is the great amount of biometric data necessary for the attack to be carried out (e.g., in a signature recognition system operating at a point with FAR=0.01%, the attacker would need to have, in average, a database comprising 10,000 different signatures to carry out a successful brute force attack). Such a big quantity of biometric samples is not easy to obtain, which has led in many cases to not consider this type of attacks as a realistic danger to the security level of the system.

However, in the past few years, several works have presented different algorithms to generate synthetic biometric traits such as fingerprints [1], iris [15], voice [4], signature [3, 7, 13] or handwriting [10]. In many cases, these synthetically generated traits have proven to present, when used in automatic recognition systems, a very similar performance to that of the real ones [2]. In addition, synthetic databases have the clear advantage over real datasets of presenting a nearly effort-free generation process in comparison to the time-consuming and complicated process of real acquisition campaigns. All these characteristics make synthetic samples very useful tools for the performance evaluation of biometric systems. However, at the same time they turn brute force attacks into a feasible security threat as they might be used to overcome the lack of biometric data by an eventual attacker.

In the present work we present an evaluation of an on-line signature verification system against a brute force attack carried out with synthetically generated handwritten signatures. The signatures are generated according to the algorithm presented in [7], which is based on the modeling of the trajectory functions in the frequency domain. Comparative results between a brute force attack carried out with real and synthetic signatures are given, proving the feasibility of executing such an attack with artificial samples.

The rest of the paper is structured as follows. An overview of the algorithm used to generate the synthetic signatures is given in Sect. 2. The protocol followed in the experiments, together with the results obtained are presented in Sect. 3. Conclusions are finally drawn in Sect. 4.

978-0-7695-3725-2/09 $25.00 © 2009 IEEE
DOI 10.1109/ICDAR.2009.39

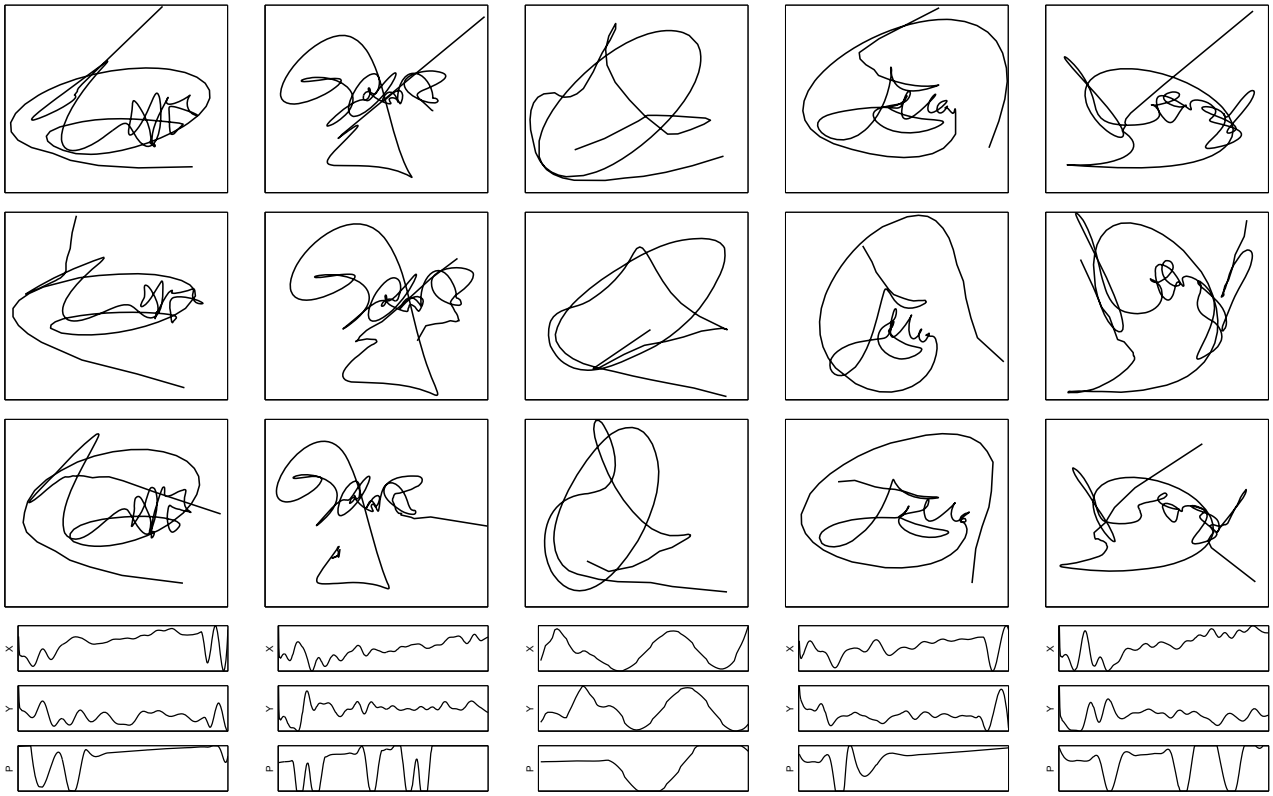

Figure 1. Synthetic signatures produced with the described generation algorithm. Three samples of five different synthetic signers are shown together with the time signals $x(t)$, $y(t)$, and $p(t)$ corresponding to the first sample.

2 Generating synthetic signatures

In the present contribution we will consider that on-line handwritten signatures are described by three time sequences, namely: i) the two trajectory functions x and y defining respectively the horizontal and vertical movement of the signing process, and ii) the pressure function p that represents the pressure exerted by the signer at each sampled point. Other dynamic information such as the azimuth or elevation angles of the writing pen will not be taken into account.

The synthetic signatures used in the experiments are generated following the algorithm described in [7]. This method follows three steps in order to generate realistic signatures starting from white noise:

- **Step 1**. A parametrical model in the frequency domain is used to colour white noise and create the synthetic Discrete Fourier Transform (DFT) of the trajectory signals x and y. The parameters that define the model are: i) time duration, ii) number of low-frequency high-energy coefficients (i.e., number of coefficients whose energy exceeds a given threshold), iii) magnitude of these relevant coefficients, iv) magnitude of the remaining DFT coefficients (high-frequency and low-energy).

- **Step 2**. The Inverse Discrete Fourier Transform (IDFT) is computed and the resulting trajectory signals are processed in the time domain in order to give the synthetic signatures a more realistic appearance. This processing stage consists of: i) smoothing of the signals, ii) giving the x signal a growing behaviour (as is the case in most left to right written signatures), iii) adding an artificial round-like flourish at the end of some signatures, iv) translation, rotation and scaling transformations.

- **Step 3**. The pressure function of the signature is generated according to the coordinate signals previously created. The penups of the signal are located close to

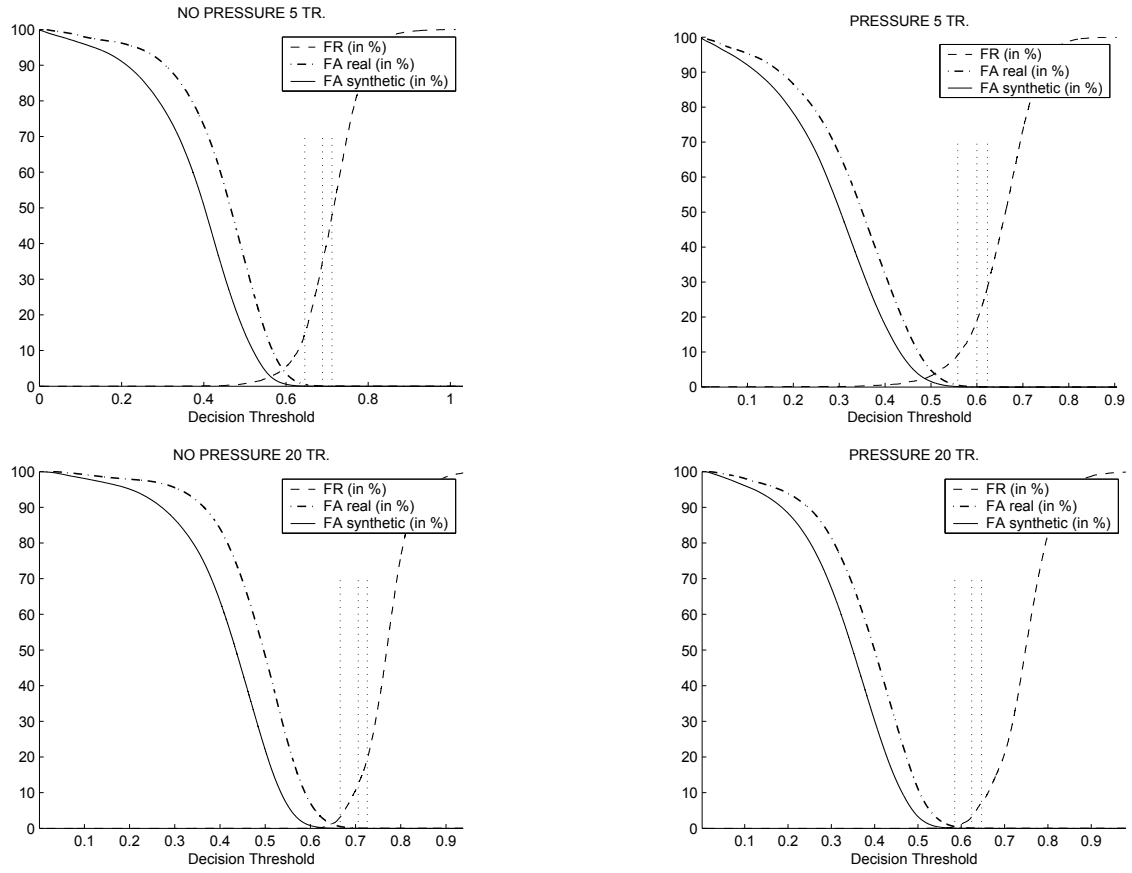

Figure 2. FRR (dashed curves), FAR with real impostors (dashed doted curves), and FAR with synthetic impostors (solid curves), for all the configurations of the system used (with and without considering the pressure function, and for 5 and 20 training signatures). The vertical doted lines correspond to the operating points with FAR (real impostors) of 0.5%, 0.05%, and 0.01%.

maxima/minima of the y function (as happens in most cases in real signatures) and undesired effects are suppressed (e.g., too long or too short penups, penups at the start or the end of the signature, etc.) The pressure signals are finally quantized to 1024 levels.

Once the three dynamic sequences (x, y, and p) have been created, different samples of that master-signature are generated modelling the user intravariability, both intrasession and intersession. The process for generating multiple samples includes: i) scaling the three functions, ii) length expansion or contraction, and iii) addition of smoothed white noise to the trajectory sequences.

In Fig. 1 some examples of synthetic signatures generated following the described algorithm are shown.

3 Experiments

3.1 Experimental Protocol

The experiments were carried out on the publicly available MCYT database [12] (comprising 8,250 real signatures samples from 330 different signers). Real signature models constructed from MCYT were attacked with a synthetically generated database following the same structure as MCYT (330 signatures $\times$ 25 samples per signature). The attacked models were constructed using the HMM-based recognition system described in [5] using a configuration of 12 left-to-right HMM states and mixtures of 4 Gaussians per state. The evaluation was carried out in four different conditions: with and without considering the pressure function, and for 5 and 20 training signatures.

A brute force attack is successful when, after a certain number of attempts, the attacker is able to enter the sys-

FAR real impostors (in %)		0.5	0.05	0.01
No Pressure	**5 Tr.**	0.04	0.001	NA
	20 Tr.	0.02	NA	NA
Pressure	**5 Tr.**	0.1	0.006	0.001
	20 Tr.	0.05	0.002	NA

Table 1. Success Rates (SRs) of the brute force attacks carried out with synthetic signatures at three different operating points of the system being attacked (decision threshold corresponding to FAR against real impostors = 0.5%, 0.05%, and 0.01%). NA means that none of the impostor matchings performed during the brute force attack broke the system.

tem using a different signature to that of the genuine user. Thus, the Success Rate (SR) of a brute force attack can be defined as $1/N$ (where N is the mean number of attempts necessary to access the system), which coincides with the False Acceptance Rate (FAR) of the system. For this reason the FAR of the evaluated system was computed under two different working scenarios:

- **Normal operation mode**. In this scenario both enrollment and test are performed with real signatures (i.e., only the MCYT database is considered). The results obtained in this scenario are used as reference. In order to compute the genuine and impostor sets of scores, the MCYT database was divided into training and test sets, where the training set comprises either 5 or 20 genuine signatures of each user (used to train the system), and the test set consists of the remaining samples, thus resulting in 330×20 or 330×5 genuine scores. Impostor scores are obtained using one signature of each of the remaining users (i.e., 330×329 impostor scores). These sets of scores are used to compute the FAR (real impostors) and FRR (False Rejection Rate) of the system.

- **Brute force attack with synthetic signatures**. In this case only impostor scores are computed, matching the trained models of real users with all the synthetic signatures generated. This results in a set of $330 \times 330 \times 25$ impostor scores, which are used to compute the FAR curve of the system when using synthetic signatures.

3.2 Results

In Fig. 2 we show the FRR (dashed curve), the FAR with real impostors (dash-doted curve) for the four configurations considered (i.e., with and without taking the pressure function into account, and for 5 and 20 training signatures) in the normal operation mode, and the FAR (solid curve) for the brute force attack using synthetic signatures. We can observe that both FAR curves (using real and synthetic signatures) present a very similar behaviour in all the range of scores.

Worth noting, the FAR curve obtained with the synthetic signatures is below the FAR curve for the normal operation mode of the system for all the operating points. This means that, as expected, the system distinguishes better between real and synthetic signatures, than in the case of considering only real signatures. However the values of both curves are quite close, proving this way the feasibility of using synthetically generated signatures to carry out this type of attack.

In Table 1 we show the quantitative results for the three operating points highlighted in Fig. 2 with vertical doted lines which correspond to FARs (i.e., using real impostors) of 0.5%, 0.05%, and 0.01% under the normal operation mode. We can observe that the difference in the Success Rates (SRs) between both attacks (i.e., with real and synthetic signatures) is around one order of magnitude. Interestingly, this difference is lower when we take into account the pressure function, which means that this information makes synthetic signatures have a more realistic appearance, so that the system has a greater difficulty in distinguishing between them and real signatures.

4 Conclusions

In this contribution we have presented an evaluation of a handwritten signature recognition system against a brute force attack carried out with synthetically generated signatures. The artificial signatures were created colouring white noise with a parametrical model of the DFTs of the trajectory functions. The experiments were carried out by attacking real signature models obtained with a HMM-based recognition system with synthetic signatures. The results show the feasibility of such a brute force attack using syn-

thetic samples.

These results stress the importance of considering this type of vulnerability when designing practical biometric security applications and encourage us to further study effective countermeasures to prevent this type of attacks.

5 Acknowledgements

J. G. is supported by a FPU Fellowship from Spanish MEC and J. F. is supported by a Marie Curie Fellowship from the European Commission. This work was supported by Spanish MEC under project TEC2006-13141-C03-03.

References

[1] R. Cappelli, A. Lumini, et al. Fingerprint image reconstruction from standard templates. *IEEE TPAMI*, 29:1489–1503, 2007.

[2] R. Cappelli, D. Maio, et al. Performance evaluation of fingerprint verification systems. *IEEE Trans. on PAMI*, 28(1):3–18, 2006.

[3] M. Djioua and R. Plamondon. A new algorithm and system for the characterization of handwriting strokes with delta-lognormal parameters. *IEEE TPAMI*, 2009. to appear.

[4] T. Dutoit. *An introduction to text-to-speech synthesis*. Kluwer Academic Publishers, 2001.

[5] J. Fierrez, J. Ortega, et al. HMM-based on-line signature verification: feature extraction and signature modeling. *Pattern Recognition Letters*, 8:2325–2334, 2007.

[6] J. Galbally, R. Cappelli, et al. Fake fingertip generation from a minutiae template. In *Proc. IAPR ICPR*, 2008.

[7] J. Galbally, J. Fierrez, et al. Synthetic generation of handwritten signatures based on spectral analysis. In *Proc. SPIE Biometric Technology for Human Identification*, 2009. to appear.

[8] J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. In *Proc. ICB*, pages 386–395. Springer LNCS-4642, 2007.

[9] A. K. Jain, P. Flynn, and A. A. Ross, editors. *Handbook of biometrics*. Springer, 2008.

[10] A. Lin and L. Wang. Style-preserving english handwriting synthesis. *Pattern Recognition*, 40:2097–2109, 2007.

[11] M. Martinez-Diaz, J. Fierrez, et al. Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification. In *Proc. IEEE ICCST*, volume 1, pages 151–159, 2006.

[12] J. Ortega-Garcia, J. Fierrez-Aguilar, et al. MCYT baseline corpus: a bimodal biometric database. *IEE Proc. VISP*, 150(6):391–401, 2003.

[13] D. V. Popel. *Synthesis and analysis in biometrics*, chapter Signature analysis, verification and synthesis in pervasive environments, pages 31–63. World Scientific, 2007.

[14] U. Uludag and A. K. Jain. Attacks on biometric systems: a case study in fingerprints. In *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI*, pages 622–633, 2004.

[15] J. Zuo, N. A. Schmid, et al. On generation and analysis of synthetic iris images. *IEEE Trans. IFS*, 2:77–90, 2007.