

픽셀 정보를 이용한 캡차 분석

서승환* 양대현**

*인하대학교 정보보호연구실

SeungHwan Seo* DaeHun Nyang**

*Information Security Research Laboratory, Inha University.

요 약

캡차는 현재 웹 서비스에서 사람과 컴퓨터를 구별하기 위해 사용되고 있고 그 사용량이 증가하는 추세이다. 이 논문에서는 아주 간단한 픽셀 정보를 이용하여 캡차를 인식하는 방법에 대해 알아보았고, 이 방법으로 현재 SK텔레콤의 공식 웹사이트인 티월드에서 사용되고 있는 캡차를 실험한 결과, 총 1,000번 중 999번을 성공하였다. 이처럼 티월드의 캡차는 픽셀 정보를 바탕으로 한 공격에 취약함이 확인되었다.

I. 서론

인간을 가장한 컴퓨터의 자동화된 공격을 막기 위해 이메일 서비스, 온라인 설문 조사, 검색 엔진 봇, 워밍 및 스팸, 사전 공격 차단, 블로그의 스팸 댓글 예방, 웹사이트 가입 등에 캡차를 사용하고 있다[1, 2]. 관련 연구로는 픽셀의 개수를 세어 캡차에 나온 문자를 판단하는 방법[3], 픽셀의 색상 정보를 이용하여 캡차의 배경을 제거하는 방법[4] 등이 있다.

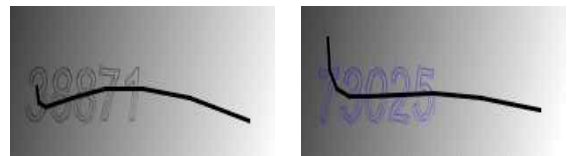
이 논문은 픽셀 정보를 이용하여 SK텔레콤 공식 웹사이트인 티월드의 캡차를 분석하였다.

이 논문은 다음과 같이 구성되어 있다. II장에서는 티월드에서 사용 중인 캡차의 특징과 캡차 분석 알고리즘에 대해서 설명한다. III장에서는 실험 환경 및 실험 결과에 대한 분석을 서술하고 IV장에서는 이 논문에 대한 결론을 내린다.

II. 티월드 캡차 분석

2.1 특징

티월드 가입, 로그인 등에 사용되는 캡차는 [그림1]과 같으며, 다음과 같은 특징을 가진다.



[그림1] 티월드에서 사용 중인 캡차

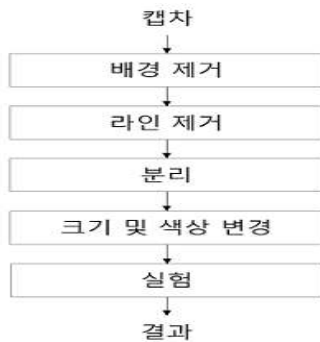
- 0에서 8까지 다섯 개의 숫자로 구성된다.
- 캡차 이미지의 크기는 300x100으로 고정된다.
- 숫자의 크기, 모양, 기울기, 숫자 사이의 간격 등은 고정되어 있지 않다.
- 모든 숫자를 관통하는 임의의 검은색 곡선이 존재한다.
- 배경의 그래데이션은 항상 동일하다.

- 숫자의 색은 검은색 혹은 파란색이다.
- 숫자는 Hollow캡차와 유사한 그림자를 가진다.

2.2 캡차 분석

2.2.1 알고리즘

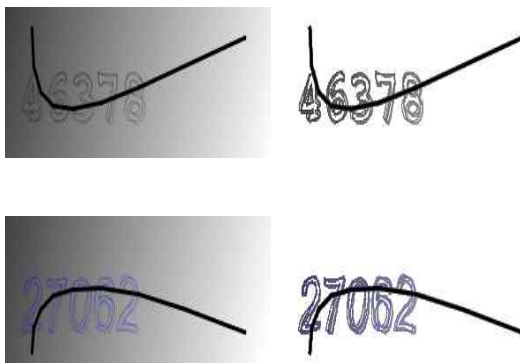
캡차 분석 알고리즘은 [그림 2]와 같다. 다운로드한 이미지를 대상으로 배경과 라인을 제거한 후 숫자별로 하나씩 나누어 분리한다. 분리된 이미지를 실험 전에 미리 생성해놓은 모델 파일을 이용하여 SVM으로 예측한다. 그리고 분리된 이미지의 예측 결과를 취합하여 최종 결과를 얻는다.



[그림 2] 알고리즘의 흐름

2.2.2 배경 제거

티월드의 경우 캡차 배경의 픽셀 정보가 항상 동일하다. 우선 배경 픽셀 정보를 분석하여 기본 배경을 생성한다. 생성해놓은 기본 배경과 받아온 캡차를 비교하면 배경이 제거된 캡차 이미지를 얻을 수 있다. [그림 3]은 배경을 제거한 캡차의 모습이다.



[그림 3] 배경을 제거한 캡차

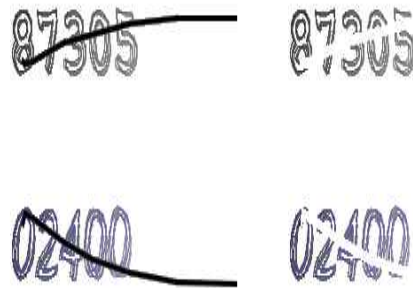
2.2.3 라인 및 얼룩 제거

티월드의 캡차는 육안으로는 구별할 수 없는 그라데이션이 있는 검은색 라인을 갖는다. 캡차 배경의 그라데이션이 항상 동일한 것과 달리 라인의 그라데이션은 캡차마다 상이하다. 아래 [그림 4]는 한 캡차의 라인을 확대한 모습이다.



[그림 4] 라인을 확대한 모습

라인을 제거하기 위해 먼저 픽셀의 색상 정보를 이용하여 색이 가장 진한 부분인 라인의 중심 위치를 찾는다. 그리고 라인의 중심에서 사방으로 확대해 가면서 픽셀의 색상 정보를 확인하고 그 값이 미리 정한 임계값 이하이면 라인으로 간주하여 제거한다. [그림 5]는 라인을 제거한 캡차의 모습이다.



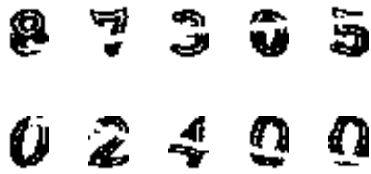
[그림 5] 라인을 제거한 캡차

2.2.4 분리

배경의 픽셀 정보를 바탕으로 수직으로 히스토그램을 그리면 어렵지 않게 분리된 이미지를 얻을 수 있다. [그림 6]는 분리된 캡차를 보여준다.

2.2.5 크기 및 색상 조정

모든 이미지의 여백과 얼룩 등은 위의 과정에서 제거되었기 때문에 이 과정에서는 정확한 실험을 위해 크기를 동일하게 조정하고, 색상 값도 동일하게 설정하였다.



[그림 6]
위의 [그림 5] 캡차를 분리하고
크기 및 색상을 조정한 결과

2.2.6 SVM을 이용한 분류

SVM(Support Vector Machine)은 분류, 회귀 및 기타 학습 작업 등에 사용되는 인기 있는 기계 학습 방법 중 하나이다[5]. SVM은 데이터를 훈련시키고 예측하는 모델을 만들어서 그것으로 데이터의 분류를 할 수 있는 도구이다. 이번 실험에는 현재 가장 널리 사용되고 있는 공개된 SVM 소프트웨어 중 하나인 LIBSVM을 사용하였다[5, 6].

분리된 이미지를 대상으로 SVM에 트레이닝을 하였다. 트레이닝 대상은 캡차 링크를 통해 얻은 1,000개의 캡차로 각 숫자의 분리 상태의 좋고 나쁨에 상관없이 모두 트레이닝 시켰다.

III. 실험

3.1 실험 환경

티월드 캡차 링크를 통해 받은 1,000개의 캡차를 사용하여 SVM 학습에 쓰일 모델을 만들었다. 모델 생성에 이용한 이미지들은 실험에 사용하지 않았으며, 캡차의 5개 숫자가 모두 일치하는 경우에만 성공한 것으로 판단하였다.

3.2 실험 결과

실험에 사용된 캡차는 총 1,000세트이며, 100세트씩 10회에 걸쳐 총 1,000번의 실험을 하였고 그 중 999번을 성공하였다. 한 번의 실패는 캡차의 숫자와 라인의 겹침이 심해 눈으로도 구별이 불가능한 경우였다.

IV. 결론

이 논문에서는 현재 티월드에서 로그인과 회원정보 변경 등에 사용되고 있는 텍스트 기반의 캡차를 분석하였다. 픽셀의 정보를 바탕으로 캡차의 문자를 쉽게 인식할 수 있었고 그 결과 티월드에서 사용 중인 캡차는 매우 취약하다는 것을 알 수 있었다. 이 논문에서 분석한 티월드의 캡차 뿐만 아니라 다음, 유폴리스 등의 캡차도 위의 방법을 사용한 결과 다음은 100%, 유폴리스는 99% 인식에 성공했다. 이와 유사한 다른 캡차들도 이러한 방법으로 쉽게 인식할 수 있을 것이다.

[참고문헌]

- [1] L. Von Ahn, M. Blum, N. Hopper, and J. Langford. "CAPTCHA: Using hard AI problems for security." *Advances in Cryptology EUROCRYPT 2003*, pages 294-311.
- [2] Carnegie Mellon University, "The Official CAPTCHA site.", <http://www.captcha.net>, 2000-2010.
- [3] Jeff Yan, Ahmad Salah El Ahmad. "Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms." *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*. pages 279-291.
- [4] Elie Bursztein, Matthieu Martin, John Mitchell. "Text-based CAPTCHA strengths and weaknesses." *CCS '11 Proceedings of the 18th ACM conference on Computer and communications security, 2011*, pages 125-138.
- [5] Chih-Chung Chang and Chih-Jen Lin, "LIBSVM : A Library for Support Vector Machines.", *ACM Transactions on Intelligent Systems and Technology*

(TIST) archive Volume 2 Issue 3, April
2011, Article No. 27.

- [6] <http://www.csie.ntu.edu.tw/~cjlin/libsvm/>,
LIBSVM.