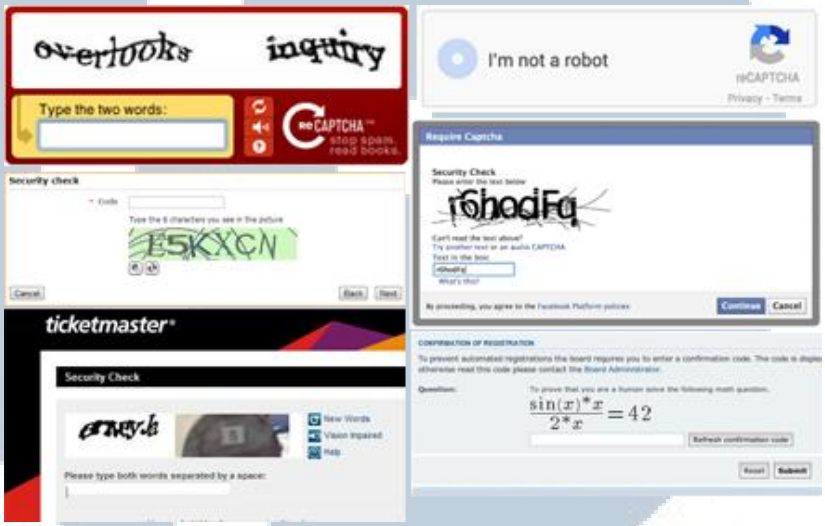
BAB II

TINJAUAN PUSTAKA

2.1. CAPTCHA



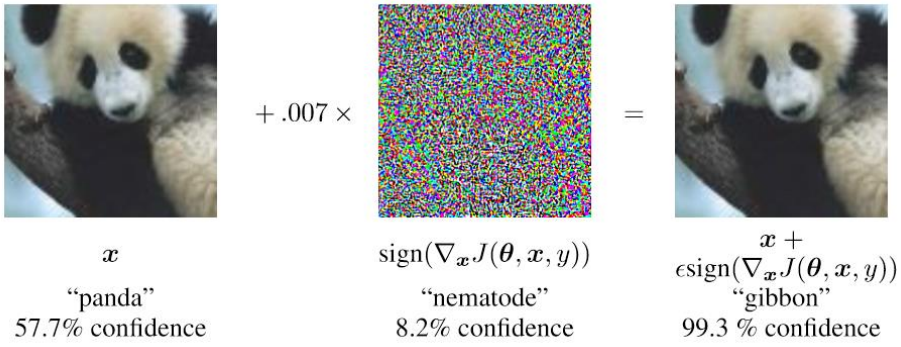
Gambar 2.1 Contoh Varian CAPTCHA [9]

Gambar 2.1 menunjukkan contoh CAPTCHA (Completely Automatic Public Turing Test to Tell Computer and Human Apart), adalah sistem yang digunakan untuk mengidentifikasi perbedaan manusia dan komputer secara otomatis. Sistem tersebut memiliki dasar pada topik-topik permasalahan Artificial Intelligence (AI) yang masih sulit diselesaikan untuk keperluan keamanan. Diharapkan bahwa sistem CAPTCHA memberikan win-win solution, dimana jika permasalahan yang digunakan belum bisa diselesaikan maka dapat digunakan sebagai sarana untuk membedakan manusia dengan komputer, dan jika terselesaikan maka menandakan kemajuan kecerdasan buatan pada topik permasalahan yang digunakan. CAPTCHA mirip dengan Turing Test, namun terdapat perbedaan dimana jurinya adalah komputer.

Tujuan utama dari sistem ini adalah mengajukan pertanyaan yang dapat dijawab dengan mudah oleh manusia, namun komputer pada masa dibuatnya CAPTCHA terkait tidak dapat menjawab pertanyaan tersebut dengan akurasi tinggi [2].

2.2. Adversarial Examples

Kemajuan di bidang Deep Learning telah mengurangi jarak kemampuan yang dimiliki oleh manusia dan komputer, yang sebelumnya dimanfaatkan oleh CAPTCHA terdahulu, seperti pengolahan suara dan pengenalan gambar. Namun meskipun tingkat akurasinya semakin mendekati kemampuan manusia, kecerdasan buatan berbasis *Deep Learning* masih memiliki kerentanan terhadap gangguan kecil pada input yang tidak disadari manusia namun dapat mengakibatkan kesalahan klasifikasi. Gangguan tersebut disebut dengan *adversarial perturbation*, dapat dibuat secara khusus untuk memaksa terjadinya kesalahan klasifikasi pada model yang digunakan kecerdasan buatan. *Adversarial examples* (*input* yang telah ditambahkan *adversarial perturbation*) yang dirancang sebagai kesalahan klasifikasi terhadap satu model kecerdasan buatan juga seringkali dapat membuat model kecerdasan buatan lain yang tidak berkaitan turut mengalami kesalahan klasifikasi [10].



Gambar 2.2 *Adversarial Examples* [13]

Gambar 2.2 adalah ilustrasi pengaplikasian *adversarial perturbation*, dimana gambar asli akan ditambahkan dengan *noise gradient* yang memiliki *alpha channel* / transparansi sangat rendah (0.007 pada ilustrasi tersebut) sehingga menghasilkan gambar akhir yang secara kasat mata tetap sama dengan gambar aslinya.

2.3. Usability Testing

Usability testing adalah sebuah proses yang mengikutsertakan sekumpulan orang sebagai partisipan tes dan merupakan representasi dari target pengguna, untuk melakukan evaluasi sampai ke tingkat sebuah produk menemui kriteria usabilitas yang spesifik. Penyertaan representasi pengguna ini adalah yang membedakan dengan evaluasi ahli, *walkthrough*, dan sebagainya yang tidak memerlukan representasi pengguna sebagai bagian dalam prosesnya. *Usability testing* adalah sebuah metode riset yang setiap pendekatan tesnya memiliki objektif yang berbeda, juga kebutuhan waktu dan sumber daya yang berbeda. [11]

Framework usability testing untuk CAPTCHA menurut Beheshti, et al. [4] terdiri dari akurasi, *response time* dan kepuasan pengguna, dimana

ketiganya dapat diukur secara kuantitatif dan kriteria tersebut dapat membantu untuk meningkatkan usabilitas dari model CAPTCHA yang digunakan. Selain itu dapat pula diuji secara spesifik usabilitas CAPTCHA berdasarkan distorsi, konten, dan presentasi dari CAPTCHA tersebut.

2.4. Penelitian Terkait

2.4.1. Adversarial Examples Pada CAPTCHA

Osadchy, M, et al. dalam publikasinya berjudul "No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation" [10] membahas tentang pembuatan *image-based* CAPTCHA yang diaplikasikan dengan *adversarial examples* untuk menghindari pengenalan gambar oleh bot. Analisis dari *proof of concept* mereka menunjukkan solusi CAPTCHA tersebut menawarkan keamanan yang tinggi dan usabilitas yang baik dibandingkan dengan CAPTCHA yang ada sebelumnya.

2.4.2. Lokalisasi CAPTCHA

"Localized CAPTCHA for illiterate people" oleh M. Shirali-Shahreza dan M. H. Shirali-Shahreza [5], "AN EXPLORATION INTO THAI INTERNET USERS' ATTITUDE TOWARDS CAPTCHA" oleh Chatpong Tangmanee dan Paradorn Sujarit-apirak [7], serta "Design of CAPTCHA Script for Indian Regional Websites" oleh M. Tariq Banday dan Shafiya Afzal Sheikh [6] merupakan

penelitian-penelitian yang menguji aspek lokalisasi di negara masing-masing (Persia, Thailand, India) terhadap usabilitas dari sistem CAPTCHA. Hasil uji coba dari penelitian-penelitian tersebut memperlihatkan penerimaan masyarakat lokal yang meningkat dan metrik usabilitas yang lebih tinggi.