

PERANCANGAN DAN PERBANDINGAN *TEXT-BASED* CAPTCHA DENGAN *IMAGE-BASED* CAPTCHA MENGGUNAKAN METODE *PROTOTYPE*

Ahmedi Firdaus

Program Studi Teknik Informatika
STMIK Indonesia Mandiri, Jl.Jakarta No.79 Bandung
Email: ahmedifirdaus@gmail.com

ABSTRAK

Keamanan sistem komputer berbasis *web* merupakan hal yang harus diperhatikan, karena sistem berbasis *web* sangat rentan terhadap tindakan kejahatan komputer. Serangan terhadap sistem tersebut banyak dilakukan dengan menggunakan program yang diotomatisasi (*bots*) yang menyamar layaknya sebagai manusia. Berdasarkan masalah tersebut diperlukan metode pengujian untuk membedakan proses validasi antara *bots* dengan manusia tetapi tetap memperhatikan kenyamanan dalam penggunaannya. Metode tersebut sering disebut dengan *reverse turing test*. CAPTCHA (*Completely Automated Public Turing test to tell Computers and Human Apart*) merupakan salah satu dari metode *reverse turing test*. Berdasarkan hasil penelitian ini menunjukkan bahwa *text-based* CAPTCHA dan *image-based* CAPTCHA dapat diimplementasikan dengan baik dan dapat menjadi solusi untuk memproteksi sistem komputer berbasis *web* dari serangan *bots*, sehingga sistem menjadi relatif lebih aman dan terhindar dari usaha-usaha penyusupan yang dilakukan oleh pihak yang tidak bertanggung jawab. Dalam pengembangan sistem CAPTCHA ini digunakan metode *prototype* dimana perubahan dan presentasi *prototype* ini dapat dilakukan berkali-kali sampai dicapai kesepakatan bentuk perangkat lunak yang akan dipakai.

Kata Kunci: *Web, Bots, CAPTCHA, sistem komputer, keamanan, Prototype.*

1. PENDAHULUAN

Perkembangan teknologi informasi terutama bidang jaringan komputer berkembang dengan pesat khususnya pengguna *Internet*. Tidak semua pengguna *Internet* dapat menghargai privasi orang lain. Banyak pengguna *Internet* yang dengan sengaja mencari keuntungan dan memanfaatkan kelemahan sistem orang lain untuk melakukan tindakan kejahatan komputer. Serangan terhadap sebuah sistem komputer kebanyakan dilakukan melalui *Internet*, serangan itu terutama dilakukan untuk

mendapatkan sesuatu sesuai dengan keinginan penyerang. Dalam *Internet* banyak program yang diotomatiskan, misalnya untuk *spam* dan membuat banyak akun palsu. Salah satu alternatif untuk menghindari serangan yang terjadi pada *Internet* menggunakan metode pengujian atau tes terhadap pengguna sistem komputer. Pengujian tersebut bertujuan mengetahui bahwa suatu sistem diakses oleh pengguna atau mesin *script* yang diotomatisasi. Pengujian ini sering dikenal dengan metode Turing Tes Terbalik (*Reverse Turing Test*). Alternatif lain yang digunakan untuk melakukan tersebut adalah dengan menggunakan CAPTCHA. Penggunaan CAPTCHA dapat menjadi solusi yang tepat, sehingga *Internet* dapat ditingkatkan keamanannya dari pihak-pihak penyerang yang tidak bertanggung jawab.

Text-based CAPTCHA dan *image-based* CAPTCHA merupakan 2 teknik dari beberapa teknik yang digunakan untuk membedakan antara *bots* dengan manusia dimana dalam implementasi tes yang dilakukannya akan menampilkan pertanyaan dalam bentuk perhitungan secara acak untuk *text-based* CAPTCHA, sedangkan *image-based* CAPTCHA akan menampilkan teks acak dalam sebuah gambar yang sudah di distorsikan.

Penelitian ini berfokus pada analisis jenis *text-based* CAPTCHA dan *image-based* CAPTCHA berdasarkan interaksi *user* dengan masing-masing jenis CAPTCHA tersebut. Untuk selanjutnya dapat ditentukan jenis CAPTCHA yang sesuai dengan tingkat kemudahan dan keamanan bagi *user* sebagai bahan rekomendasi untuk pengembang *website*.

Usability dan *Security* merupakan dua aspek yang mendasar pada CAPTCHA dan saling berhubungan tetapi seringkali berlawanan satu sama lain. Jika suatu *interface* didesain semakin aman maka akan menyebabkan penggunaan yang kurang nyaman. Sedangkan jika suatu *interface* didesain lebih nyaman dalam penggunaannya maka akan menyebabkan *interface* tersebut kurang aman (Sauer. 2010).

1.1. Rumusan Masalah

Berdasarkan latar belakang yang diuraikan diatas, sehingga dapat dirumuskan beberapa permasalahan yang ada, yaitu:

- a) Bagaimana cara mengetahui perbandingan antara *text-based* CAPTCHA dengan *image-based* CAPTCHA?
- b) Bagaimana mencegah dan mengurangi serangan oleh *bot*?
- c) Manakah yang lebih baik dari segi kemudahan dalam penggunaannya bagi *user* dan keamanannya dalam melindungi *website* dari serangan *bot* antara *text-based* CAPTCHA dengan *image-based* CAPTCHA?

1.2. Tujuan Penelitian

Adapun tujuan dari penelitian ini:

- a) Mengetahui perbandingan antara *text-based* CAPTCHA dengan *image-based* CAPTCHA.
- b) Menjadikan CAPTCHA sebagai solusi untuk memproteksi sistem komputer berbasis *web* dari serangan *bot* sehingga sistem menjadi relatif lebih aman dan terhindar dari usaha-usaha penyusupan yang dilakukan oleh pihak yang tidak bertanggung jawab.
- c) Memberikan kemudahan bagi *user* menggunakan CAPTCHA dalam mengakses *website* dan menjaga keamanan *website* dari serangan *bot*.

2. LANDASAN TEORI

2.1. Keamanan Web

Keamanan *web*, sangat erat kaitannya dengan jaringan, karena untuk mengakses sebuah *website* pasti dibutuhkan koneksi jaringan. Saat ini sangat pesat sekali perkembangan teknologi *website*, jaringan dan bermacam ancaman keamanan yang dihadapi, seperti ancaman terhadap kerahasiaan yang sering dihadapi adalah *hacker*, *Masquerader*, *virus-virus* dari internet maupun dari media transfer data seperti *flasdisk*, *hardisk eksternal*, melalui jaringan LAN, *download file* tanpa proteksi, *Trojan horse*, aktifitas *user* yang tidak terotorisasi dan masih banyak lagi ancaman keamanan yang kadang tidak kita sadari (Satriadi, 2012).

2.2. CAPTCHA

CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) adalah suatu bentuk uji tantangan–tanggapan (*challenge – response test*) yang digunakan dalam perkomputeran untuk memastikan bahwa jawaban tidak dihasilkan oleh suatu komputer. Proses ini biasanya melibatkan suatu komputer (*server*) yang meminta seorang pengguna untuk menyelesaikan suatu uji sederhana yang dapat dihasilkan dan dinilai oleh komputer tersebut. Karena komputer lain tidak dapat memecahkan CAPTCHA, pengguna manapun yang dapat memberikan jawaban yang benar akan dianggap sebagai manusia. Oleh sebab itu, uji ini kadang disebut sebagai uji Turing balik (*Reverse Turing test*), karena dikelola oleh mesin dan ditujukan untuk manusia, kebalikan dari uji Turing standar yang biasanya dikelola oleh manusia dan ditujukan untuk suatu mesin. CAPTCHA umumnya menggunakan huruf dan angka dari citra terdistorsi yang muncul dilayar (Kaur, 2014).

2.2.1. Text-based CAPTCHA

Text-based CAPTCHA merupakan teknik CAPTCHA yang menggunakan teks yang pada dasarnya tidak ada variasi sehingga tes yang dilakukan untuk membedakan manusia atau komputer dilakukan dengan teks secara acak atau *random*. Semua pertanyaan yang diajukan akan ditampilkan dalam teks acak sehingga dapat meminimalisir adanya celah untuk *bots* melakukan serangan guna memecahkan kode CAPTCHA yang diberikan. *Text-based* CAPTCHA memiliki desain yang cukup mudah dipahami dibandingkan dengan jenis CAPTCHA lainnya (Mahato, 2015).

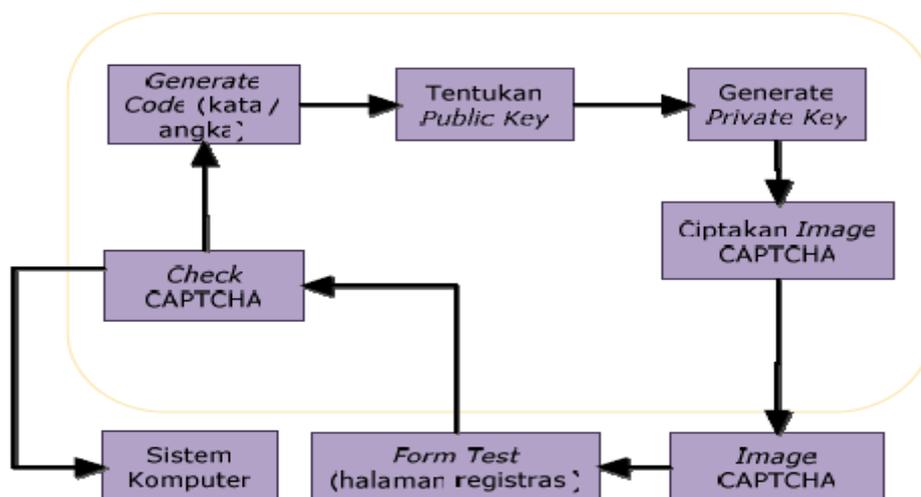
2.2.2. Image-based CAPTCHA

Image-based CAPTCHA memiliki beberapa variasi, yang paling umum digunakan saat ini adalah simbol yang dimiringkan dan dimunculkan pada sebuah gambar dan pengenalan bentuk. CAPTCHA yang menggunakan simbol dimiringkan yang dimunculkan pada gambar disebut Gimpy, EZ Gimpy adalah varian dari Gimpy, Pessimial Print dan Bufflext. Gimpy pertama kali dikembangkan oleh Luis Von Ahn dari Carnegie Mellon University yang mendesain versi paling sederhana dari Gimpy,

disebut EZ-Gimpy. Ez-Gimpy yang sekarang ini digunakan oleh Yahoo! Dan suatu versi serupa digunakan oleh Hotmail. Perbedaan yang mendasar antara Gimpy dan EZ-Gimpy adalah Gimpy memiliki tiga atau lebih kata yang dimiringkan yang dimunculkan pada suatu gambar, sedangkan EZ-Gimpy hanya memiliki satu kata yang dimiringkan pada suatu gambar (Aulia, 2013).

2.3. Sistem Kerja CAPTCHA

CAPTCHA digunakan untuk memproteksi suatu situs *web*. Gambar berikut ini menggambarkan cara kerja CAPTCHA secara umum:



Gambar 2.1. Cara Kerja CAPTCHA (Fikry, 2016)

Berikut penjelasan gambar sistem kerja CAPTCHA:

1. Rangkaian kode di-*generate* berupa huruf dan angka atau sebuah kata, kemudian suatu *image-based CAPTCHA* di-*generate* berdasarkan rangkaian kode tersebut. Sesuai dengan algoritma *public key cryptography* akan di-*generate private key* yang hanya dapat berpasangan dengan rangkaian kode yang dihasilkan tersebut (*public key*).
2. *Private key* akan di-*render* sebagai *hidden field* pada *form*, dan harus ada *input box* yang akan menerima masukan dari pengguna berupa *public key* atau *image CAPTCHA* yang ditampilkan.

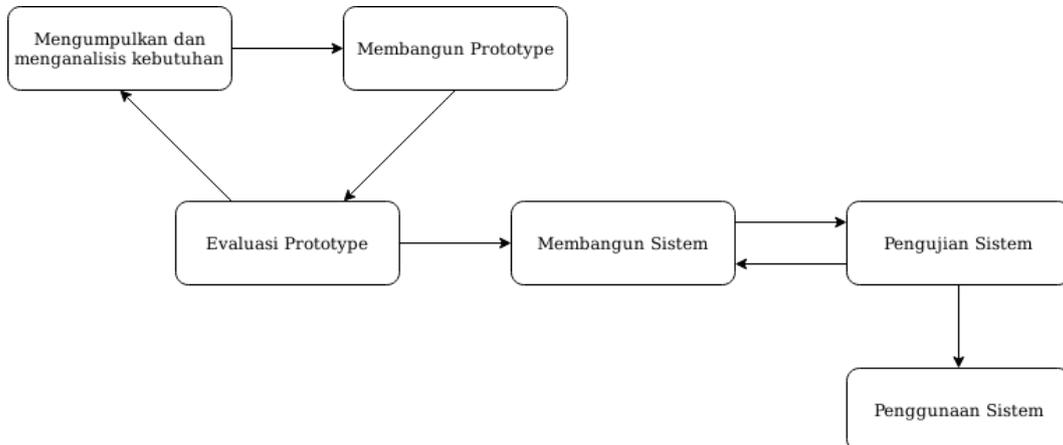
3. *Private key* dan *public key* yang akan di-*submit* oleh pengguna kemudian dibandingkan oleh sistem dengan algoritma *public key cryptography*. Jika ada kecocokan, berarti CAPTCHA sah dan jika tidak ada kecocokan, berarti ada indikasi yang melakukan *submit* bukan manusia.

2.4. Metode Pengembangan Perangkat Lunak

Metode pengembangan sistem pada penelitian ini menggunakan metode *prototype* yaitu, metode pengembangan perangkat lunak yang memodelkan sistem kerja suatu perangkat lunak yang belum lengkap atau berupa *prototype* kepada pihak *user* (O'Brien, 2005).

Prototype dari perangkat lunak yang dihasilkan kemudian dipresentasikan kepada *user* dan diberikan kesempatan untuk memberikan masukan-masukan sehingga perangkat lunak yang dihasilkan nantinya benar-benar sesuai dengan keinginan dan kebutuhan *user*.

Berikut ini adalah tahapan metode *Prototype*:



Gambar 1.1. Tahapan Metode *Prototype* (O'Brien, 2005)

- a) Mengumpulkan dan menganalisis kebutuhan.

Sebelum memulai pekerjaan yang bersifat teknis, sangat diperlukan untuk mengumpulkan kebutuhan dan data-data yang diperlukan dan menganalisis kebutuhan tersebut demi memahami dan mencapai tujuan yang ingin dicapai.

Pengumpulan data-data tambahan bisa juga diambil dari artikel, jurnal, dan *internet*.

b) Membangun sebuah *prototype*.

Pada tahapan kedua ini dibuat sebuah *prototype* dari sistem yang akan dibangun, tetapi *prototype* ini hanya di fokuskan pada penyajian kepada *user*. Tujuannya supaya *user* lebih memahami gambaran besar dari sistem yang akan dibangun.

c) Evaluasi *prototype*.

Tahap berikutnya adalah tahap evaluasi pada *prototype* yaitu dengan cara menerima umpan balik dari *user* supaya sistem yang nantinya akan dibangun dapat berjalan dengan baik dan sesuai dengan kebutuhan.

d) Membangun sistem.

Setelah menerima umpan balik dari *user* maka pada tahapan ini akan dilakukan implementasi dan pembangunan sistem yang sesungguhnya.

e) Pengujian program.

Pada tahapan ini dilakukan pengujian pada sistem yang sudah utuh dan siap pakai. Pengujian dilakukan untuk mengetahui *error* pada sistem sebelum sistem tersebut digunakan.

f) Menggunakan Sistem.

Sistem sudah selesai dan siap untuk digunakan.

3. PERANCANGAN

3.1. Mengumpulkan dan Menganalisis Kebutuhan

3.1.1. Pengumpulan Data

Pengumpulan data merupakan langkah yang dilakukan peneliti untuk mendapatkan data-data yang berkaitan dengan CAPTCHA untuk mendukung penelitian ini yang sedang dilakukan peneliti. Teknik pengumpulan data yang dilakukan dalam penelitian ini adalah dengan studi literatur dan studi lapangan.

3.1.2. Menganalisis Kebutuhan

Agar penelitian ini dapat berjalan dengan lancar, maka dibutuhkan sumber daya yang diperlukan untuk menjalankan tahapan dengan baik. Kebutuhan yang dimaksud adalah kebutuhan mengenai data-data dan sumber daya yang dibutuhkan dalam penelitian, seperti kebutuhan akan perangkat keras dan perangkat lunak untuk menjalankan sistem yang dibangun.

3.1.2.1. Analisis CAPTCHA

Dalam membangun CAPTCHA dilakukan beberapa tahapan analisis:

1. Informasi menentukan masalah yang akan dibangun sistem CAPTCHA nya.
2. Mengumpulkan data yang diperlukan untuk membangun sistem berupa jenis-jenis, ciri-ciri, dan penjelasan CAPTCHA melalui studi literatur, studi lapangan, dan penelitian.
3. Mempresentasikan pengetahuan yang didapat.
4. Menentukan target *user* yang akan menggunakan CAPTCHA.

3.1.2.2. Analisis Identifikasi Masalah

Analisis masalah merupakan langkah dimana langkah ini diperlukan untuk mengetahui permasalahan yang akan terjadi di dalam sistem yang sedang dirancang oleh penulis. Identifikasi masalah pada penelitian ini adalah cara mengetahui perbandingan antara *text-based* CAPTCHA dan *image-based* CAPTCHA dan manakah yang lebih baik dari segi kemudahan dan keamanannya serta mencegah serangan oleh *bot*.

3.1.2.3. Analisis Pengguna

Agar penggunaan sistem dapat berjalan secara optimal dan sesuai dengan yang diharapkan, maka dibutuhkan kemampuan untuk bisa menjalankan sistem CAPTCHA yang dirancang oleh peneliti. Dalam hal ini, kemampuan tersebut terutama adalah harus terbiasa menggunakan perangkat komputer dan telah mengenal CAPTCHA.

3.1.2.4. Analisis Perangkat Keras

Analisis kebutuhan perangkat keras dimaksudkan untuk mengetahui spesifikasi perangkat keras yang dibutuhkan pada penelitian ini. Berikut kebutuhan perangkat keras pada penelitian ini:

- a) *Processor* dengan kecepatan minimal 1GHz + *Motherboard*
- b) RAM minimal 512 MB
- c) *Hard disk* minimal 10 GB
- d) *Monitor*
- e) *Mouse*
- f) *Keyboard*

Secara keseluruhan spesifikasi perangkat keras semua yang ada sudah memenuhi syarat untuk kebutuhan penelitian ini.

3.1.2.5. Analisis Perangkat Lunak

Perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut:

- a) Sistem Operasi Kali GNU/Linux.
- b) Apache sebagai *server*.
- c) Sublime Text sebagai *editor*.
- d) *Web browser* yang digunakan untuk menampilkan CAPTCHA.

Berdasarkan analisis perangkat lunak yang telah dijelaskan diatas sebagian besar sudah mencukupi untuk dapat menjalankan aplikasi yang akan dirancang.

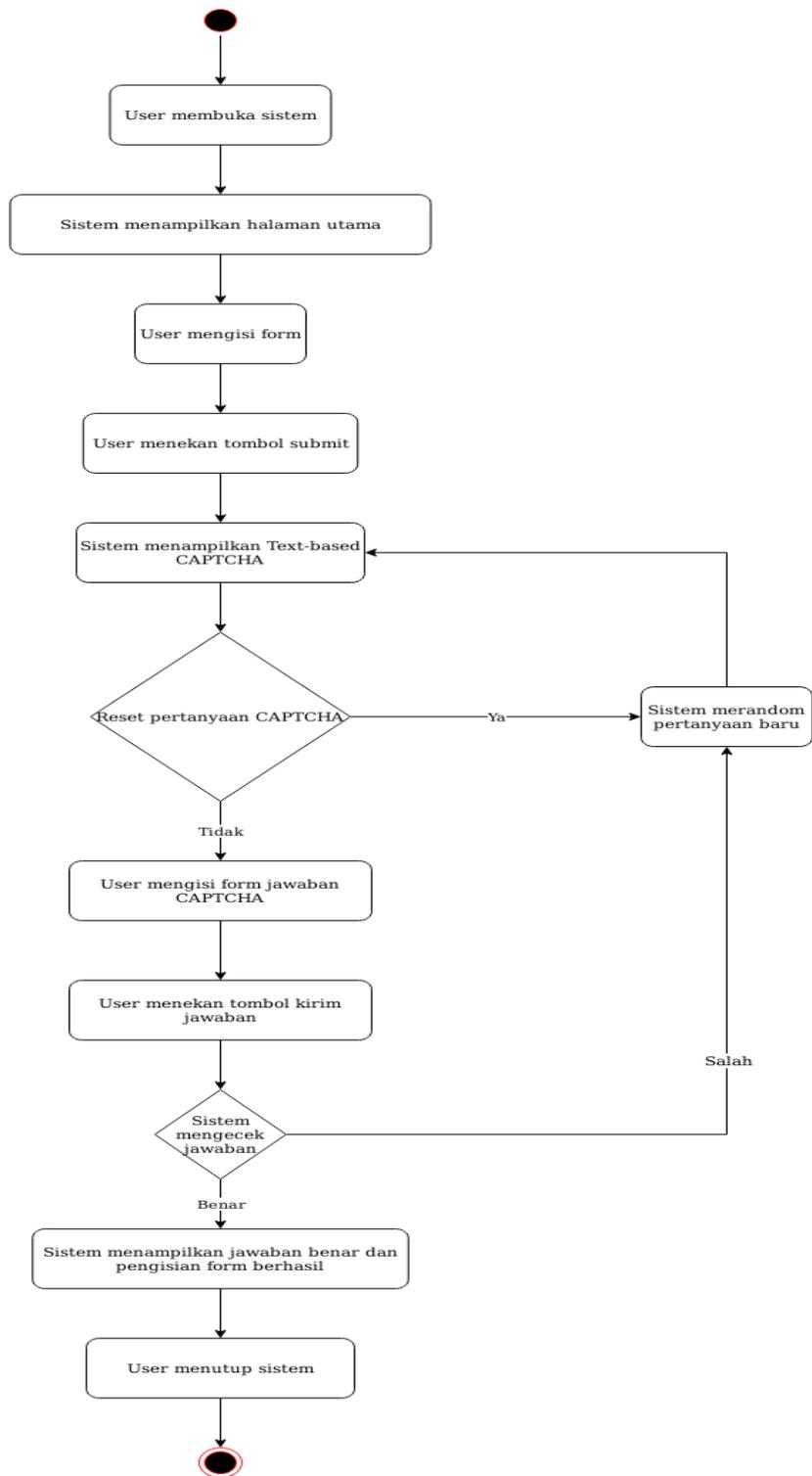
3.2. Membangun *Prototype*

Pada penelitian ini akan menggunakan CAPTCHA dengan jenis *text-based* dan *image-based* yang nantinya akan dibandingkan dari segi kemudahan dan keamanannya. *Text-based* CAPTCHA merupakan teknik CAPTCHA yang menggunakan teks yang pada dasarnya tidak ada variasi sehingga tes yang dilakukan untuk membedakan manusia atau komputer dilakukan dengan teks secara acak atau *random*. Berikutnya adalah CAPTCHA yang memiliki beberapa variasi yaitu *image-based* CAPTCHA, yang

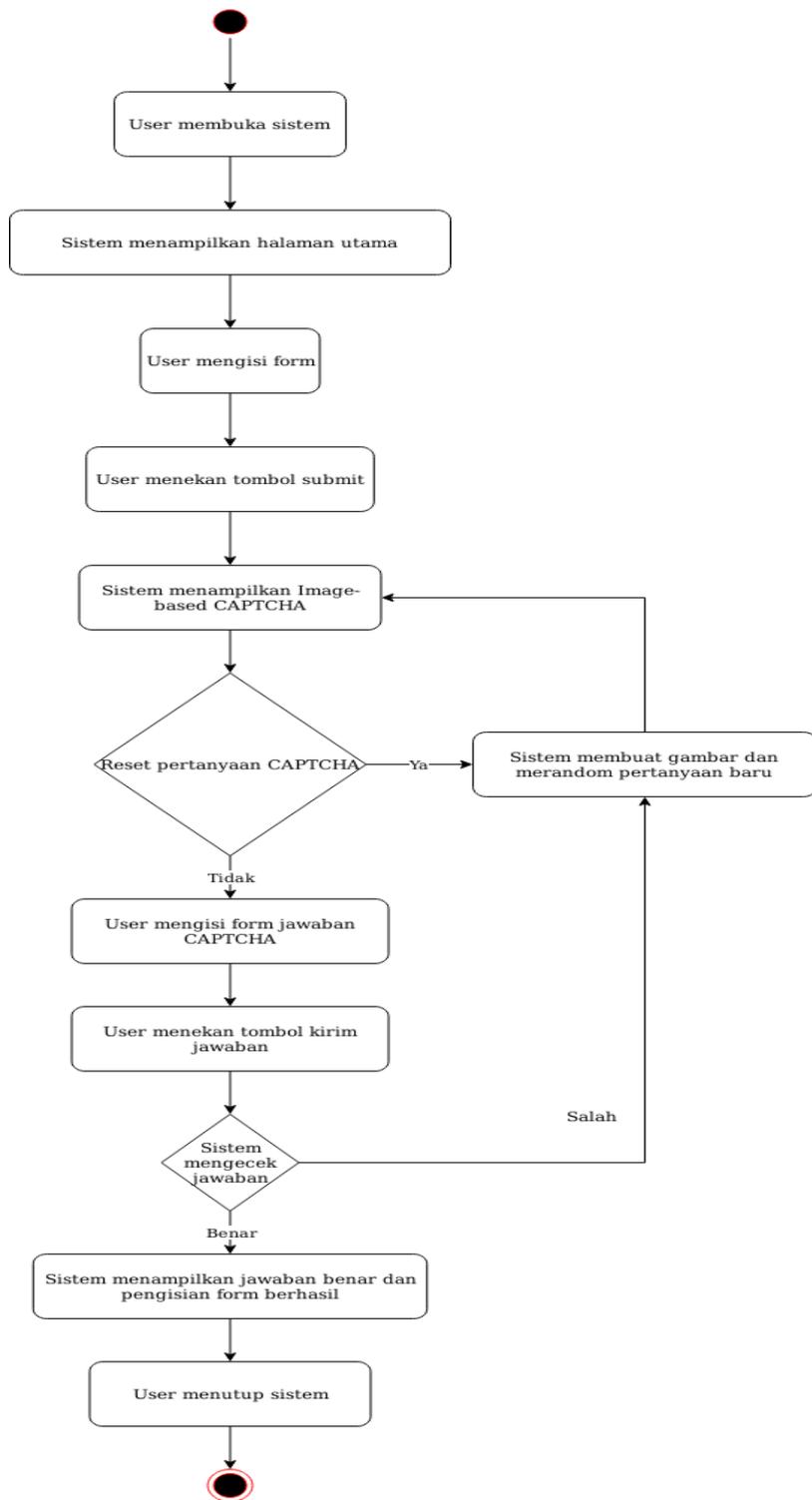
paling umum digunakan saat ini adalah simbol yang dimiringkan dan dimunculkan pada sebuah gambar.

3.2.1. Perancangan Model *Prototype*

Perancangan ini bertujuan untuk memenuhi kebutuhan penelitian mengenai gambaran yang jelas tentang perancangan sistem yang akan dirancang. Dalam perancangan model, penulis akan menggunakan *flowchart* untuk menggambarkan cara kerja dari *text-based* CAPTCHA dan *image-based* CAPTCHA. Perancangan sistem dari *text-based* CAPTCHA dengan *image-based* CAPTCHA ini memiliki cara kerja yang mirip, hanya berbeda dari apa yang ditampilkannya. *Text-based* CAPTCHA akan menampilkan pertanyaan dalam bentuk perhitungan, sedangkan *image-based* CAPTCHA akan menampilkan pertanyaan dalam bentuk gambar yang sudah didistorsikan. Berikut alur kerjanya:



Gambar 3.1. Alur Kerja dari *Text-based* CAPTCHA



Gambar 3.2. Alur Kerja dari *Image-based* CAPTCHA

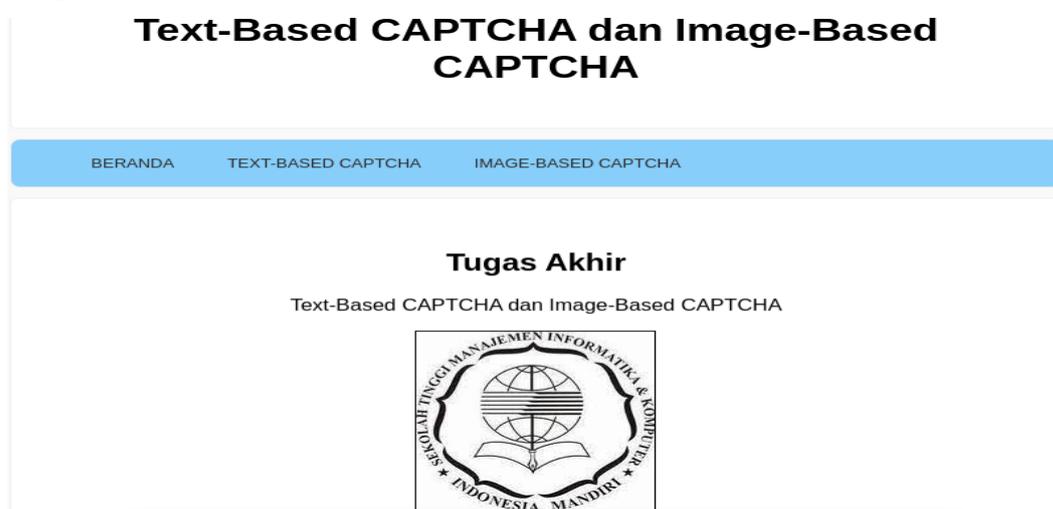
3.2.2. Implementasi *Prototype*

Setelah tahap perancangan model *prototype* selesai, maka selanjutnya penulis akan membangun model *prototype* dari *text-based* CAPTCHA dan *image-based* CAPTCHA yang nantinya akan diuji untuk mengetahui perbandingannya. Berikut ini adalah implementasi *prototype text-based* CAPTCHA dan *image-based* CAPTCHA:

1. Captcha_text.php. File ini menampilkan *text-based* CAPTCHA.
2. class-captcha.php. File ini berisikan langkah kerja pembentukan pertanyaan yang ditampilkan pada *text-based* CAPTCHA.
3. Captcha_image.php. File ini menampilkan *image-based* CAPTCHA.
4. image.php. File ini berisikan proses pembuatan tes yang ditampilkan pada *image-based* CAPTCHA, mencakup pembuatan gambar, penambahan garis, dan titik yang digunakan untuk mendistorsikan gambar.
5. index.php. File yang menampilkan halaman awal atau beranda.

Tampilan dari hasil implementasi *prototype text-based* CAPTCHA dan *image-based* CAPTCHA sebagai berikut:

1. Tampilan beranda



Gambar 3.8. Tampilan Menu Awal/Beranda

2. Tampilan *prototype text-based* CAPTCHA

Text-Based CAPTCHA dan Image-Based CAPTCHA



The screenshot shows a web application interface with a blue navigation bar at the top containing the links "BERANDA", "TEXT-BASED CAPTCHA", and "IMAGE-BASED CAPTCHA". Below the navigation bar, the page is titled "Login". There are two input fields: "Username :" and "Password :". Below the password field, the section is titled "Text-Based CAPTCHA". The question is "Berapa hasil dari 4 - 5 ?" followed by an empty input field. There are two buttons: "Submit" and "RESET".

Gambar 3.9. Tampilan dari *Prototype Text-based* CAPTCHA

3. Tampilan *prototype image-based* CAPTCHA

Text-Based CAPTCHA dan Image-Based CAPTCHA



The screenshot shows a web application interface with a blue navigation bar at the top containing the links "BERANDA", "TEXT-BASED CAPTCHA", and "IMAGE-BASED CAPTCHA". Below the navigation bar, the page is titled "Login". There are two input fields: "Username :" and "Password :". Below the password field, the section is titled "Image-Based CAPTCHA". The image shows a distorted text "0 V U Z 7" with a horizontal line through it. There are two buttons: "SUBMIT" and "RESET".

Gambar 3.10. Tampilan dari *Prototype Image-based* CAPTCHA

3.3. Evaluasi *Prototype*

Berdasarkan masukan-masukan yang diterima oleh penulis dari *user*, maka akan dilakukan beberapa perubahan pada CAPTCHA. Berikut ini adalah perubahan yang akan dilakukan pada CAPTCHA:

1. Melakukan perubahan pada desain, yaitu dengan menambahkan beberapa variasi pada tampilan CAPTCHA.
2. Menambah jenis perhitungan pada tes di *text-based* CAPTCHA, karena jenis perhitungan yang saat ini ada pada tes di *prototype text-based* CAPTCHA ada 2 jenis yaitu penjumlahan dan pengurangan. Pada tahap selanjutnya akan ditambahkan perhitungan dengan jenis perkalian.
3. Menambah distorsi gambar pada tes di *image-based* CAPTCHA, karena distorsi yang ada pada tes di *prototype image-based* CAPTCHA saat ini terlalu sedikit sehingga ada kemungkinan CAPTCHA dapat ditembus oleh *bot*.

4. IMPLEMENTASI DAN UJI COBA

4.1.1. Implementasi

Implementasi *text-based* CAPTCHA dan *image-based* CAPTCHA dilakukan berdasarkan hasil analisis, perancangan CAPTCHA, dan hasil evaluasi pada pembahasan sebelumnya. Sehingga diharapkan CAPTCHA ini dapat mencapai tujuan yang diinginkan.

4.1.1.1. Lingkungan Implementasi

Lingkungan implementasi untuk pembangunan *text-based* CAPTCHA dan *image-based* CAPTCHA ini mencakup *hardware* (perangkat keras) dan *software* (perangkat lunak). Berikut adalah rincian lingkungan implementasi yang digunakan:

1. *Hardware*
 - a) *Processor* : Intel(R) Atom(TM) CPU N2600 @ 1.60GHz
 - b) *Memory* : 2 GB
 - c) *Hard disk* : 320 GB
2. *Software*

- a) Sistem Operasi : Kali GNU/Linux
- b) *Web Server* : Apache 2.0
- c) *Web browser* : Google Chromium

4.1.1.2. Hasil Implementasi

Setelah tahap analisis dan perancangan model selesai dan didapat hasil evaluasi, maka selanjutnya penulis akan membangun model dari *text-based* CAPTCHA dan *image-based* CAPTCHA yang nantinya akan diuji untuk mengetahui perbandingannya. Berikut ini adalah implementasi *text-based* CAPTCHA dan *image-based* CAPTCHA:

1. *Captcha_text.php*. File ini menampilkan *text-based* CAPTCHA.
2. *class-captcha.php*. File ini berisikan langkah kerja pembentukan pertanyaan yang ditampilkan pada *text-based* CAPTCHA.
3. *Captcha_image.php*. File ini menampilkan *image-based* CAPTCHA.
4. *image.php*. File ini berisikan proses pembuatan tes yang ditampilkan pada *image-based* CAPTCHA, mencakup pembuatan gambar, penambahan garis, dan titik yang digunakan untuk mendistorsikan gambar.
5. *index.php*. File yang menampilkan halaman awal atau beranda.

Hasil implementasi tampilan *text-based* CAPTCHA dan *image-based* CAPTCHA yang sudah diperbaharui sebagai berikut:

1. Tampilan beranda

Reservation

- [Submit](#)

Gambar 4.1. Tampilan Menu Awal/Beranda

2. Tampilan *text-based* CAPTCHA

BERANDA
Text-Based CAPTCHA
Isilah CAPTCHA dibawah ini untuk melanjutkan pemesanan
Berapa hasil dari 4 x 4 ?

Gambar 4.2. Tampilan dari *Text-based* CAPTCHA

3. Tampilan *image-based* CAPTCHA



Gambar 4.3. Tampilan dari *Image-based* CAPTCHA

4.2. Pengujian

Pengujian dilakukan untuk mengetahui apakah *text-based* CAPTCHA dan *image-based* CAPTCHA dapat mencapai tujuan yang diinginkan dan menemukan kesalahan-kesalahan yang mungkin terjadi pada bagian implementasi.

4.2.2. Pengujian *Blackbox*

Tahap pengujian *blackbox* dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Pengujian dibagi dua yaitu pengujian menampilkan CAPTCHA dan pengujian sistem. Pengujian ini dilakukan setelah CAPTCHA berhasil diintegrasikan pada *website*. Pengujian menampilkan CAPTCHA dilakukan untuk melihat hasil pembangunan dan antarmuka agar sesuai dengan hasil analisis. Pada pengujian sistem terdapat dua skenario, yaitu:

1. Skenario Normal

Skenario ini digunakan untuk menguji CAPTCHA dengan memasukkan jawaban yang benar. Hasil yang diharapkan dari pengujian ini adalah *user* bisa melakukan *submit* dengan sukses.

2. Skenario Alternatif

Skenario ini digunakan untuk menguji CAPTCHA dengan memasukkan jawaban dengan salah. Hasil yang diharapkan dari pengujian ini adalah *user* gagal melakukan *submit*.

Setelah dilakukan pengujian dengan menggunakan dua skenario di atas, maka masing-masing skenario menghasilkan hasil yang sesuai dengan harapan dari tiap-tiap skenario.

4.2.3. Pengujian UAT (*User Acceptance Test*)

Pengujian ini difokuskan kepada *feedback* pengguna terhadap CAPTCHA yang telah dibangun. Dari hasil pengujian akan mendapatkan penilaian pengguna dari faktor kemudahan dan kesulitan yang dihadapi saat melakukan penyelesaian CAPTCHA. Berikut beberapa kemungkinan situasi pengujian yang dapat dilakukan pada penelitian ini adalah:

1. Keakurasian jawaban, yaitu tingkat ketepatan pengguna dalam menjawab tes CAPTCHA.
2. Rata-rata waktu yang diperlukan pengguna untuk menyelesaikan tes CAPTCHA.

4.2.4. Pengujian Keamanan

Pengujian ini difokuskan kepada keamanan CAPTCHA terhadap berbagai serangan yang umum terjadi pada CAPTCHA. Metode serangan yang akan diuji adalah *OCR attack (Optical Character Recognition)* dan *simple brute force*. *OCR attack* yang dimaksudkan di sini adalah penggunaan *tools OCR* untuk mengambil dan mengidentifikasi karakter-karakter yang terdapat pada CAPTCHA. Sedangkan

pengujian *simple brute force* yaitu dengan menggunakan langkah paksa dalam proses *submit* CAPTCHA.

4.2.5. Analisis Hasil Pengujian

Pada akhirnya penelitian ini menghasilkan data-data mengenai *text-based* CAPTCHA dan *image-based* CAPTCHA melalui pengujian *blackbox*, kemudahan, dan keamanan. Pengujian *blackbox* dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Untuk mendapatkan data dari segi kemudahan, dilakukan pengujian menggunakan UAT yang difokuskan kepada *feedback* pengguna terhadap CAPTCHA yang telah dibangun. Terakhir, dilakukan pengujian OCR dan *simple brute force* untuk mendapatkan data dari segi keamanan.

Setelah melalui tahapan penelitian, pembuatan model dan pengujian, terdapat beberapa kelebihan dan kekurangan pada *text-based* CAPTCHA dan *image-based* CAPTCHA. Berikut adalah perbandingan kelebihan dan kekurangan dari CAPTCHA yang dibangun pada penelitian ini:

Tabel 4.1. Perbandingan *Text-based* CAPTCHA dengan *Image-based* CAPTCHA

Kategori	Tipe CAPTCHA	
	<i>Text-based</i> CAPTCHA	<i>Image-based</i> CAPTCHA
Tampilan (<i>Interface</i>)	Sederhana	Mempunyai banyak variasi
Keamanan	Tidak dapat ditembus oleh <i>Simple Brute Force</i>	Tidak dapat ditembus oleh <i>Simple Brute Force</i> dan OCR
Waktu rata-rata dalam menyelesaikan CAPTCHA	15,4 detik	23,6 detik

Tabel 4.2. Perbandingan *Text-based* CAPTCHA dengan *Image-based* CAPTCHA dari Ketepatan *User* Dalam Mengisi Jawaban CAPTCHA

Ketepatan <i>User</i> Dalam Mengisi Jawaban CAPTCHA			
Tipe CAPTCHA	Berhasil	Gagal	Hasil
<i>Text-based</i> CAPTCHA	60	0	100%
<i>Image-based</i> CAPTCHA	48	12	80%

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan apa yang telah dijelaskan pada bab-bab sebelumnya dan atas jawaban dari masalah yang telah diketahui sebelumnya, maka dapat diambil kesimpulan sebagai berikut:

1. *Text-based* CAPTCHA dan *image-based* CAPTCHA merupakan 2 teknik dari beberapa teknik yang digunakan untuk membedakan antara *bots* dengan manusia dimana dalam implementasi tes yang dilakukannya akan menampilkan pertanyaan dalam bentuk perhitungan secara acak untuk *text-based* CAPTCHA, sedangkan *image-based* CAPTCHA akan menampilkan teks acak dalam sebuah gambar yang sudah di distorsikan. Kedua CAPTCHA ini memiliki kemiripan dalam tes yang dilakukannya, tetapi juga memiliki beberapa perbedaan. Pengujian UAT (*User Acceptance Test*), OCR (*Optical Character Recognition*), dan *Simple brute force* pada masing-masing CAPTCHA dimaksudkan untuk mencari dan mengetahui apa saja perbedaan pada kedua CAPTCHA tersebut..
2. Dalam *Internet* banyak program yang diotomatiskan atau *bot*, misalnya untuk *spam* dan membuat banyak akun palsu. Salah satu alternatif untuk menghindari serangan yang terjadi pada *Internet* menggunakan metode pengujian atau tes terhadap pengguna sistem komputer. Pengujian tersebut bertujuan mengetahui

bahwa suatu sistem diakses oleh pengguna atau mesin *script* yang diotomatisasi. Penggunaan CAPTCHA dapat menjadi solusi yang tepat, sehingga *Internet* dapat ditingkatkan keamanannya dari pihak-pihak penyerang yang tidak bertanggung jawab.

3. *Usability* dan *security* merupakan dua aspek yang mendasar pada CAPTCHA dan saling berhubungan tetapi seringkali berlawanan satu sama lain. Jika suatu *interface* didesain semakin aman maka akan menyebabkan penggunaan yang kurang nyaman. Sedangkan jika suatu *interface* didesain lebih nyaman dalam penggunaannya maka akan menyebabkan *interface* tersebut kurang aman. Dalam hal ini adalah *text-based* CAPTCHA lebih mudah dan nyaman digunakan oleh *user* karena memiliki *interface* atau tampilan yang sederhana daripada *image-based* CAPTCHA. Disisi lain, *image-based* CAPTCHA memiliki banyak variasi karena dapat menambahkan distorsi pada tesnya sehingga *image-based* CAPTCHA ini lebih aman dan kemungkinan *bots* dapat menerobosnya sangat kecil.

5.2. Saran

Dengan adanya kesimpulan diatas, ada beberapa saran yang dapat dikemukakan sebagai bahan pertimbangan lebih lanjut guna meningkatkan produktifitas kerja dari CAPTCHA ini.

1. CAPTCHA ini dapat digunakan oleh masyarakat luas untuk mengamankan *website* mereka dari serangan yang dilakukan oleh *bots*.
2. Untuk keamanan yang lebih baik disarankan untuk menggunakan *image-based* CAPTCHA karena memiliki banyak variasi yang dapat diterapkan pada CAPTCHA ini.
3. Diharapkan data yang digunakan pada penelitian selanjutnya lebih banyak dikarenakan tindak kejahatan *cybercrime* yang menggunakan *bots* akan menjadi lebih banyak lagi sehingga data yang dihasilkan akan lebih baik lagi.

6. DAFTAR PUSTAKA

- Aulia, H. (2013). *Rancang Bangun Image Based CAPTCHA Terintegrasi Dengan Jigsaw Puzzle Menggunakan HTML5*, Universitas Islam Negeri Sultan Syarif Kasim Riau, 69 halaman.
- Fikry, M., & Iskandarsyah, M. (2016). *Completely Automated Public Turing Test to Tell Computers and Human Apart (CAPTCHA) Menggunakan Pendekatan Drag and Drop*. Universitas Islam Negeri Sultan Syarif Kasim Riau, 64-70.
- Gregorius. (2000). *Pengertian Web Menurut Para Ahli - Sejarah, Jenis, dan Manfaat*. <https://www.gurupendidikan.co.id/pengertian-website/>. Diakses 20 Juni 2020.
- Indrajani. (2001). *Analisis dan Perancangan Sistem Berorientasi Objek*. Bandung: Informatika.
- Jogiyanto, H.M. (2005). *Analisis dan Desain Sistem Informasi*. Yogyakarta: Andi.
- Kaur, K., & Behal, S. (2014). *Captcha and Its Techniques. A Review*. (IJCSIT) International Journal of Computer Science and Information Technologies.
- Mahato, S., Saxena, V. P., & Bhavsar, D. (2015). *A Survey of Captcha based Web and Application Security Methods and Techniques*. HCTL Open International Journal of Technology Innovations and Research (IJTIR).
- Mahato, S., Saxena, V. P., & Mishra, R. G. (2015). *Securing Web Service and Applications Using Captcha Security*. HCTL International Journal of Technology and Research (IJTIR).
- Murdick, R. G. (1991). *Sistem Menurut Para Ahli*. <https://pelajaran.co.id/2018/09/pengertian-sistem-menurut-para-ahli-terlengkap.html>. Diakses 16 Juni 2020.
- Nidhra, & Dondeti. (2012). *Pengujian Software*. <https://repository.dinamika.ac.id/id/eprint/>. Diakses 20 Juni 2020.
- O'Brien. (2005). *Metode Prototype Dalam Pembangunan Sistem Informasi*. [https://www.academia.edu/10561240/Metode Prototyping Dalam Pembangunan Sistem Informasi](https://www.academia.edu/10561240/Metode_Prototyping_Dalam_Pembangunan_Sistem_Informasi). Diakses 4 Mei 2020.

- Quadri, & Farooq. (2010). *Pengujian Software*.
<http://repository.dinamika.ac.id/id/eprint/>. Diakses 20 Juni 2020.
- Ramdhani. (2003). *Internet Menurut Para Ahli*.
<https://dosenit.com/jaringankomputerinternet/>. Diakses 20 Juni 2020.
- Riadi, I. (2008). *Optimalisasi Keamanan Website Menggunakan CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Human Apart)*. Universitas Ahmad Dahlan Yogyakarta.
- Satriadi, B. A. (2021). *Keamanan Web*. <https://www.unpas.ac.id/keamanan-web/>.
Diakses 16 Juni 2020.
- Setiawan, E. B. (2012). *Optimalisasi Keamanan Website Menggunakan CAPTCHA-AD Video*. Universitas Komputer Indonesia Bandung.
- Sulaiman, M. T., & Hassan, N. F. (2017). *Generate Random Arabic Characters and Numbers for CAPTCHA*. Iraqi Journal of Science.
- Wu, H., & Zhao, L. (2012). *Web Security A WhiteHat Perspective*. China: House of Electronics Industry.
- Yilmaz, S., Zavrak, S., & Bodur, H. (2015). *Distinguishing Human from Automated Programs by a novel Audio-based CAPTCHA*. International Journal of Computer Applications.