IMPLEMENTASI PERMAINAN FLOW PADA PEMBANGUNAN SISTEM CAPTCHA

Indra Setiawan[1] indra.setiawan@ti.ukdw.ac.id
Willy Sudiarto Raharjo[2] willysr@ti.ukdw.ac.id
Budi Susanto[3] budsus@ti.ukdw.ac.id

Abstract

The basic challenge in designing an obfuscating CAPTCHAs is to make them easy enough that users are not dissuaded from attempting a solution, yet still too difficult to solve using available image-based computer vision algorithms. CAPTCHA has been widely used in many web applications and there has been so many research on CAPTCHA. Current technology enables computer to easily solve image-based CAPTCHA with high probability, so we propose another type of CAPTCHA-based authenticaton that can not be solved by utilizing Optical Character Recognition but still easy to use for new users. We implemented the new model of CAPTCHA using FLOW game. We found that the success rate of this new system is 92.025%, completion time is 6.3614s, and 81,67% of users are able to solve it in less than 10s.

Keywords : *Authentication, CAPTCHA, Character Recognition.*

1. Pendahuluan

Spam, pendaftaran otomatis, dan pemungutan suara secara online merupakan serangan-serangan dari computer (*bot*) yang menyebabkan pemborosan sumber daya dari sebuah situs. Penyerangan dari computer (*bot*) dapat dilakukan ribuan hingga jutaan kali sehingga dapat merubah hasil dari pemungutan suara (kuisioner) sederhana atau menyebabkan banyak *account* palsu atau tidak valid.

CAPTCHA (*Completely Automated Public Turing test to tell Computer and Human Apart*) merupakan sebuah tes uji coba berdasarkan *Turing Test* yang dapat dengan mudah dipecahkan oleh manusia tetapi tidak bisa dipecahkan dengan mudah oleh komputer (*bot*). Dengan memanfaatkan CAPTCHA, pendaftaran secara otomatis atau pemalsuan suara pada proses voting tidak dapat dilakukan oleh komputer (*bot*). Saat ini, terdapat beberapa metode CAPTCHA seperti *text-based* CAPTCHA, *image-based* CAPTCHA dan *audio-based* CAPTCHA.

Untuk menjaga agar *bot* tidak bisa memasuki sistem, CAPTCHA terus dikembangkan sehingga semakin menyulitkan komputer untuk memecahkannya selagi tetap mempertahankan kondisi bahwa manusia normal harus bisa memecahkannya dengan mudah. Dalam penelitian ini, penulis mengembangkan sebuah model CAPTCHA dalam bentuk sebuah permainan berbasis FLOW yang mudah digunakan oleh pengguna. Parameter yang akan digunakan untuk mengukur adalah waktu penyelesaian dan juga jumlah kegagalan dari percobaan yang ada.

2. Teori Pendukung

2.1. *Access Control*

Access Control didefinisikan sebagai "A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy" (Shirey, 2007). Dalam

[1] Program Studi Teknik Informatika, Universitas Kristen Duta Wacana, Yogyakarta
[2] Program Studi Teknik Informatika, Universitas Kristen Duta Wacana, Yogyakarta
[3] Program Studi Teknik Informatika, Universitas Kristen Duta Wacana, Yogyakarta

implementasinya, terdapat dua komponen utama, yaitu *authentication* dan *authorization* (Stamp, 2011). Penelitian ini akan berfokus pada *authentication*.

2.2. *Authentication*

Authentication adalah sebuah proses untuk menentukan apakah seorang pengguna diijinkan untuk mengakses sebuah sistem. Secara teknis, terdapat dua kemungkinan penerapan metode *authentication*, yaitu dimana pengguna hendak masuk ke mesin komputer yang bersifat lokal dan yang melalui jaringan komputer.

Pada penerapan *authentication* melalui jaringan komputer, maka diperlukan adanya suatu aturan yang baku yang disebut dengan protokol. Protokol memungkinkan dua atau lebih aplikasi untuk berkomunikasi menggunakan aturan yang sama. Beberapa protokol *authentication* yang umum digunakan: CHAP, EAP, Kerberos, LAN Manager / NTLM, OpenID, RADIUS, dan PAP.

2.3. CAPTCHA

CAPTCHA adalah sebuah program yang bisa menghasilkan sebuah pengujian yang dapat diselesaikan oleh sebagian besar pengguna manusia, namun tidak dapat diselesaikan oleh program komputer (Ahn, 2003). Program ini dapat digunakan untuk membedakan manusia dari komputer dan memiliki banyak kegunaan terutama untuk alasan keamanan, seperti: pemungutan suara *online*, layanan email gratis, *bot search engine*, *Worms* dan *Spam*.

Bentuk implementasi sederhana dari CAPTCHA adalah sebuah gambar yang mengandung karakter atau teks tertentu yang harus dijawab oleh pengguna. Karena pengguna manusia bisa melihat teks dengan mudah, maka diasumsikan pengguna akan bisa menyelesaikan tugas (*task*) dengan mudah. Bagi komputer, tugas ini akan sangat susah untuk dilakukan karena komputer tidak memiliki panca indra yang dapat membaca teks tersebut. Contoh sederhana dari implementasi CAPTCHA pada Facebook dapat dilihat pada Gambar 1.

Implementasi CAPTCHA sangatlah bervariasi. Tim riset Microsoft membuat implementasi dari CAPTCHA yang disebut dengan Asirra (Elson, Douceur, Howell, Saul, 2007). Pengguna akan diberikan sekumpulan gambar dan diminta untuk memilih gambar yang masuk kedalam kategori tertentu. Contoh Asirra dapat dilihat pada Gambar 2.

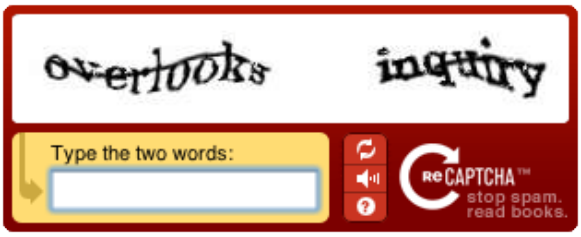
Banyak penelitian membuktikan bahwa CAPTCHA sudah tidak lagi aman. Salah satunya adalah yang dilakukan oleh Elie Bursztein, Matthieu Martin, and John C. Mitchell dari Stanford University yang menyatakan bahwa mereka menemukan 13 dari 15 layanan penyedia CAPTCHA yang ada rentan terhadap *automated attacks* (Bursztein, 2011).

Gambar 1. CAPTCHA pada Facebook

Gambar 2. Asirra

2.4. reCAPTCHA

reCAPTCHA merupakan salah satu bentuk model *authentication* berbasis *challenge-response* yang dikembangkan oleh Luis von Ahn, Benjamin Maurer, Colin McMillen, David Abraham, dan Manuel Blum pada tahun 2008. Model ini merupakan pengembangan lebih lanjut dari konsep CAPTCHA. reCAPTCHA akan meminta pengguna untuk menyelesaikan sebuah tugas (*task*) yaitu memasukan dua kata yang dimunculkan dalam bentuk gambar yang terdistorsi. Model reCAPTCHA dapat dilihat pada Gambar 3.



Gambar 3. reCAPTCHA

reCAPTCHA telah digunakan lebih dari 40.000 *website* dan orang-orang sudah bisa menggunakan dan menyelesaikan reCAPTCHA dengan mudah. Pada pengujian reCAPTCHA yang telah dilakukan oleh Luis von Ahn, Benjamin Maurer, Colin McMillen, David Abraham, dan Manuel Blum, dari 67,87% dari data yang tersedia hanya dibutuhkan dua responden saja untuk bisa menjawab dengan benar, 17,86% dari data hanya membutuhkan tiga responden, 7,10% dari data hanya membutuhkan empat responden, 3,11% dari data hanya membutuhkan lima responden, dan hanya 4,06% dari data yang membutuhkan lima atau lebih responden. Selain itu, juga dilakukan pengujian waktu dalam menyelesaikan CAPTCHA konvensional dan reCAPTCHA dengan mengambil 1000 pengguna secara acak dan menghasilkan waktu rata-rata 13,51 detik untuk CAPTCHA konvensional serta 13,06 detik untuk reCAPTCHA (Ahn, 2008)

Ahmad Basheer Hassanat melakukan pengujian CAPTCHA pada 6 muridnya dengan masing-masing 10x percobaan dan percobaan dilakukan untuk mesin OCR pada waktu yang sama. Hasil dari percobaan tersebut adalah 89,58% keberhasilan pada mesin OCR dan 83,75% keberhasilan pada manusia. Pada hasil penelitian tersebut, CAPTCHA berdasarkan dengan image tidak menutup kemungkinan dapat diselesaikan oleh mesin OCR dan jika CAPTCHA dibuat untuk menyulitkan komputer, juga akan menyulitkan seorang manusia. (Hassanat, 2014)

2.5. DevilTyper

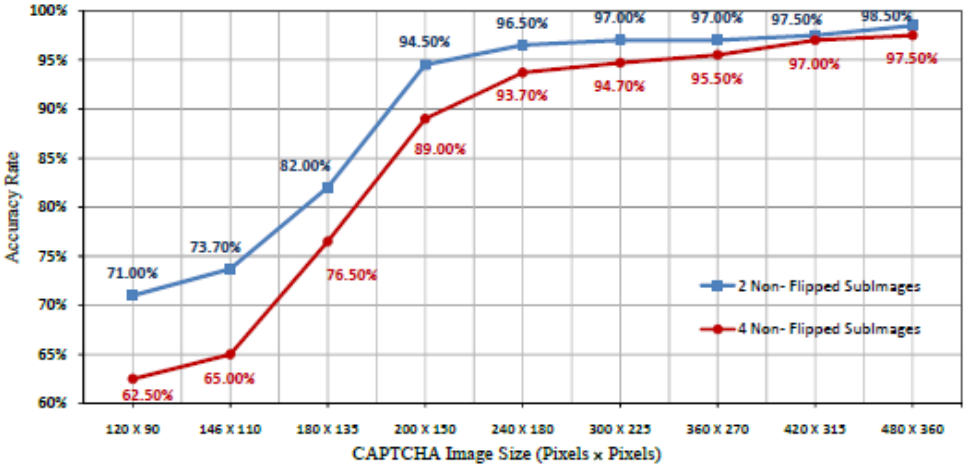
DevilTyper merupakan CAPTCHA berbasis game yang didesain untuk 1 orang pemain dimana CAPTCHA akan keluar bersama dengan sebuah monster dan pemain harus mengetikkan kata yang muncul agar pemain dapat mengalahkan monster tersebut. Sistem CAPTCHA yang digunakan DevilTyper masih menggunakan text-based dengan menambahkan skor dan ranking setelah pemain menyelesaikan. CAPTCHA DevilTyper ditunjukan pada gambar 4

Pada proses pengumpulan data selama 4 minggu didapatkan lebih dari 1.400.000 pengguna yang dapat memecahkan CAPTCHA model DevilTyper ini dengan tingkat kegagalan kurang dari 0.15%. (Ho, 2011)

Penelitian CAPTCHA berbasis gambar klik merupakan teknik sederhana dan menghasilkan keamanan terhadap serangan web otomatis. Dengan menggunakan teknik "Image Flip", keakuratan dari CAPTCHA meningkat dan waktu yang digunakan semakin sedikit. Penelitian ini mengambil pengguna sebanyak 225 orang dan menguji tingkat keberhasilan dari sistem CAPTCHA berbasis Image ini dalam hal kecepatan pengerjaannya. Tingkat keberhasilan dalam penggunaan dan kecepatan dalam menyelesaikan ditunjukkan pada gambar 5 dan 6 (Shah, 2009)

Gambar 4. CAPTCHA DevilTyper

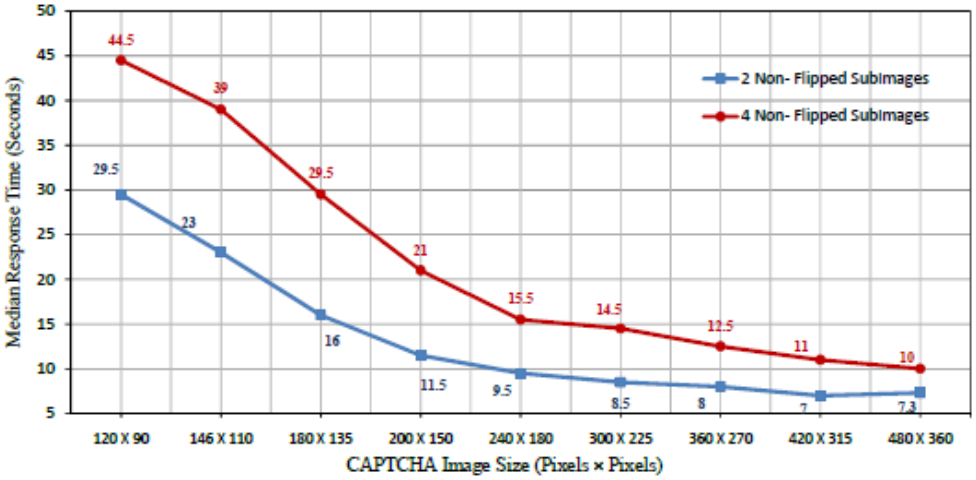
Sumber : (Ho, 2011)



Gambar 5. Tingkat keberhasilan dengan menggunakan CAPTCHA Image

Sumber : (Shah, 2009)

Gambar 5 menunjukkan tingkat keberhasilan CAPTCHA image dengan pengujian 2 gambar dengan resolusi 120x90 pixel hingga 480x160 pixel dengan menggunakan 2 dan 4 gambar. Pada penelitian dihasilkan semakin besar image yang digunakan akan menghasilkan tingkat keberhasil yang semakin tinggi. Pada image yang menggunakan 120x90 pixel hanya didapatkan 71% (pada 2 gambar) dan 62,5% (pada 4 gambar), image yang menggunakan 480x160 pixel menghasilkan keberhasilan hingga 98,5% (pada 2 gambar) dan 97,7% (pada 4 gambar)



Gambar 6. waktu tanggapan yang dibutuhkan CAPTCHA Image

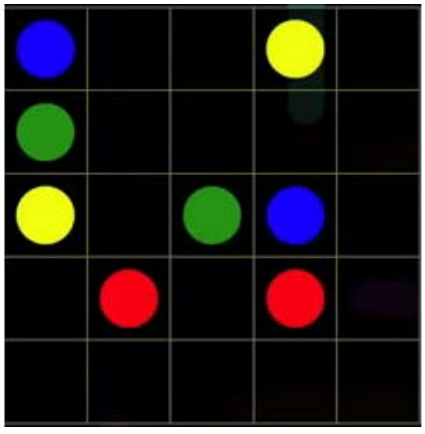
Sumber : (Shah, 2009)

Gambar 6 menunjukan waktu yang digunakan dalam mengerjakan CAPTCHA Image yang dilakukan pada dengan resolusi 120x90 pixel hingga 480x160 pixel dengan menggunakan 2 dan 4 gambar. Pada penelitian dihasilkan semakin besar image yang digunakan hanya membutuhkan waktu yang semakin sedikit. Pada image yang menggunakan 120x90 pixel membutuhkan waktu 29.5 detik (pada 2 gambar) dan 44.5s (pada 4 gambar), image yang menggunakan 480x160 pixel hanya membutuhkan 7.3 detik (pada 2 gambar) dan 10 detik (pada 4 gambar)

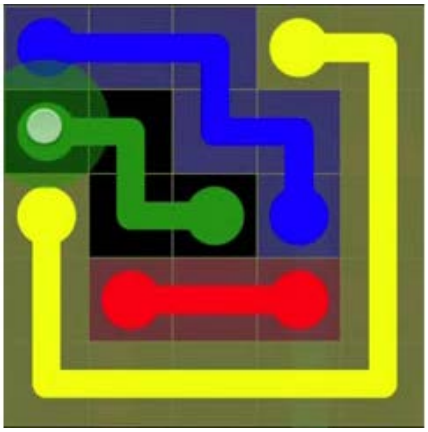
3. Perancangan Sistem

3.1. Perancangan Sistem

Peneliti menggunakan konsep permainan FLOW untuk mengembangkan sebuah model sistem authentikasi berbasis CAPTCHA. Permainan Flow adalah permainan puzzle sederhana yang menghubungan dan mencocokan warna/bentuk/gambar dengan sebuah garis. Seorang pengguna harus dapat menghubungkan 2 buah gambar dengan panduan yang sudah ada. Gambar 7 dan 8 menggambarkan kondisi awal permainan FLOW dan penyelesaiannya.

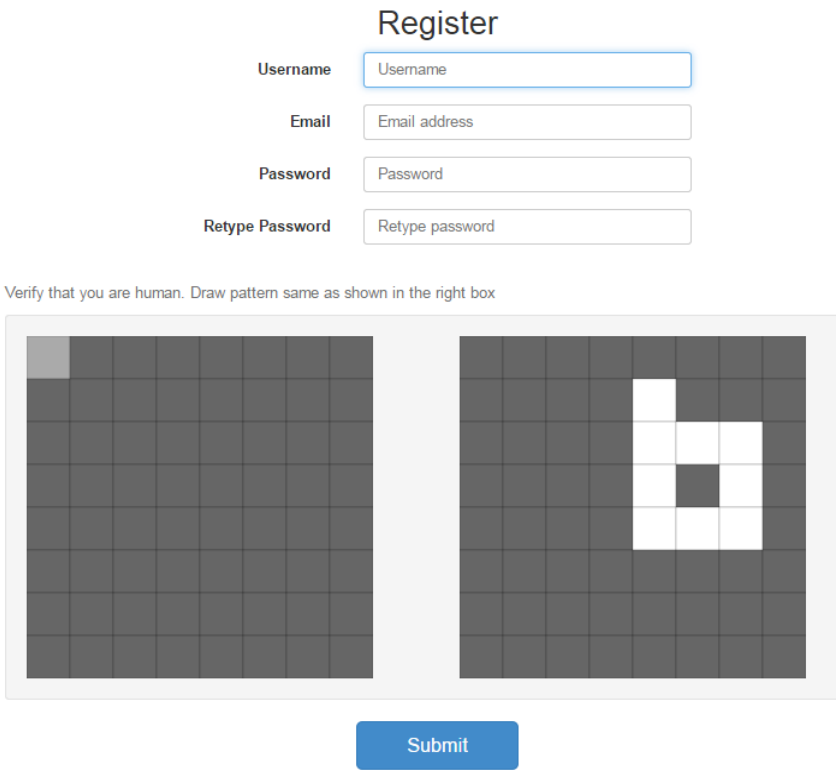


Gambar 7. Kondisi awal permainan FLOW



Gambar 8. Penyelesaian permainan FLOW

Model CAPTCHA yang dibangun berbentuk kotak sebanyak 8x8. Untuk bisa masuk kedalam sistem, pengguna harus menggambarkan pola sesuai dengan permintaan di sisi kanan yang diberikan oleh sistem secara acak dengan menggunakan operasi *click and drag* yang akan dikonversikan oleh sistem menjadi angka-angka kemudian dikirimkan oleh sistem menuju *web service*. Untuk proses pertukaran data, digunakan format data JSON yang dienkripsi dengan menggunakan CryptoJS[4] versi 3.1.2. Tampilan aplikasi ini terlihat pada Gambar 9.



Gambar 9. Aplikasi CAPTCHA berbasis permainan FLOW

[4] https://code.google.com/p/crypto-js/

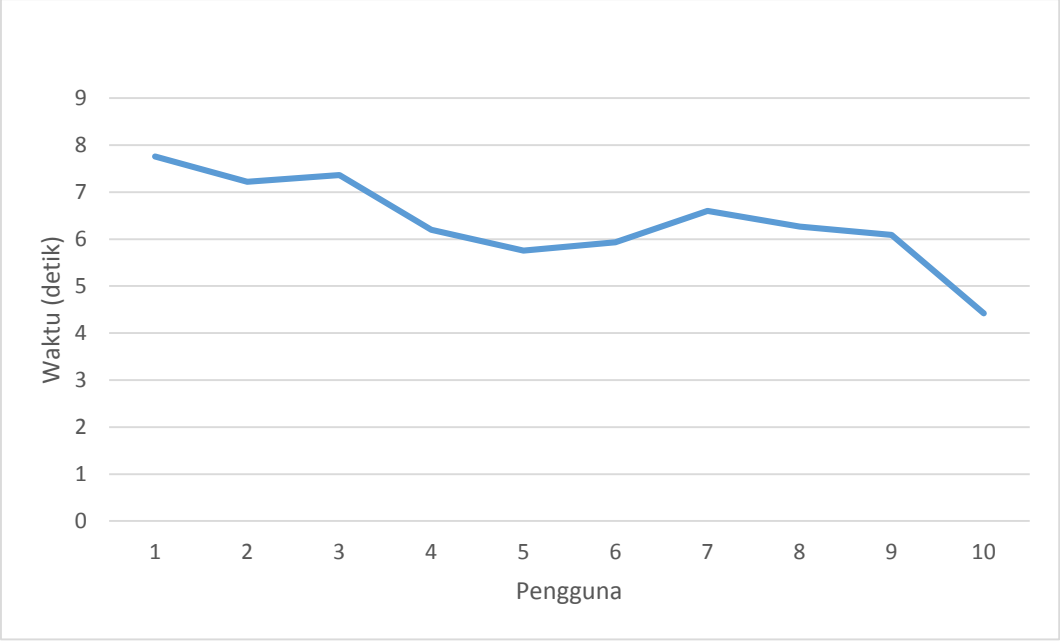
3.2. Metodologi Pengujian

Fokus dalam penelitian ini adalah bagaimana membangun sebuah model CAPTCHA yang mudah untuk digunakan oleh pengguna. Untuk bisa mengetahuinya, maka parameter yang akan digunakan adalah waktu penyelesaian dan juga jumlah kegagalan dari percobaan yang dilakukan. Waktu penyelesaian yang digunakan sebagai acuan agar bisa dianggap berhasil adalah kurang dari 10 detik. Jumlah kegagalan digunakan untuk mengetahui apakah pengguna bisa menyelesaikan tugas pada bidang yang terbatas dan dengan mengikuti pola yang sudah ditentukan oleh sistem secara acak.

Dalam penelitian ini pengujian dilakukan oleh 30 orang yang berbeda dengan masing masing menyelesaikan CAPTCHA sebanyak 10 kali setiap orangnya dengan data yang selalu acak (*random*). Pada setiap percobaan akan dihitung waktu penyelesaian dan juga berapa kali melakukan kesalahan dalam menyelesaikan percobaan.

4. Hasil Dan Pembahasan

Berdasarkan dari 300 kali pengujian CAPTCHA dihasilkan 245 waktu penyelesaian yang dapat diselesaikan kurang dari 10 detik sedangkan 55 waktu penyelesaian diselesaikan lebih dari 10 detik. Prosentase waktu penyelesaian kurang dari 10 detik adalah sebesar 81,67% dan waktu rata-rata pengguna menyelesaikan CAPTCHA adalah 6,3614 detik. Data hasil waktu rata-rata pengguna untuk menyelesaikan permainan flow dapat dilihat pada Gambar 10 sedangkan data untuk 300 pengujian secara lengkap ditampilkan pada Tabel 1.



Gambar 10. Grafik waktu rata-rata pengguna menyelesaikan permainan flow

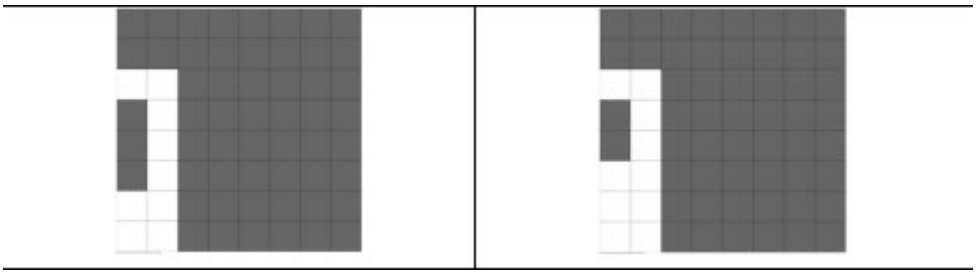
Tabel 1.
Hasil pengujian sistem berdasarkan waktu penyelesaian

User	Waktu Percobaan Ke-									
	1	2	3	4	5	6	7	8	9	10
1	7,441	7,269	4,72	2,801	3,236	3,136	4,223	4,193	4,709	3,094
2	20,036	8,784	6,187	7,978	7,767	5,318	7,502	15,211	5,028	8,662
3	22,198	15,587	9,477	7,795	10,847	16,48	7,08	6,618	7,208	4,734
4	6,05	5,88	6,769	19,528	5,757	5,862	10,724	8,05	8,578	7,018
5	23,23	7,309	21,896	8,794	3,398	9,998	6,073	40,449	11,882	6,05
6	17,902	10,654	3,852	3,729	6,318	3,785	2,466	3,759	2,851	5,016

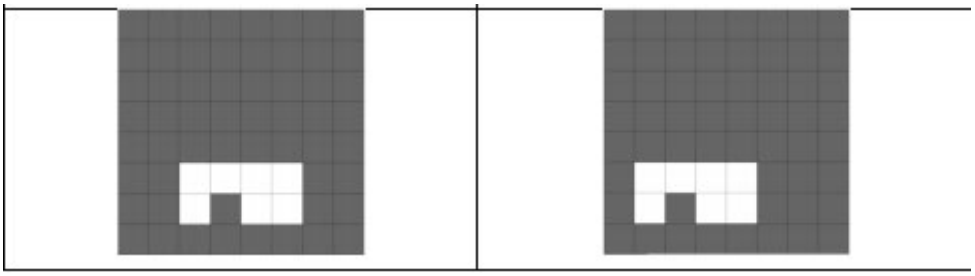
User	Waktu Percobaan Ke-									
	1	2	3	4	5	6	7	8	9	10
7	4,093	10,353	7,867	3,603	5,735	5,137	3,848	3,204	6,004	2,826
8	25,257	4,536	3,293	3,217	3,801	5,287	7,585	3,473	4,298	3,817
9	6,141	5,518	4,633	3,72	3,988	3,531	1,825	4,4	4,29	3,484
10	8,36	13,066	24,288	3,153	5,916	2,735	2,424	11,783	5,977	8,72
11	7,001	4,374	21,654	4,422	5,822	3,022	5,676	3,934	3,192	3,774
12	9,601	16,713	5,167	13,106	6,634	7,517	8,312	10,726	31,339	6,61
13	7,801	4,513	3,039	5,979	4,552	2,577	4,713	3,713	4,839	4,72
14	6,049	8,614	3,811	7,16	4,738	12,569	5,488	5,264	4,916	3,346
15	9,455	3,851	3,455	2,458	4,474	2,561	5,058	7,02	1,82	9,31
16	12,241	2,988	4,601	11,329	6,084	3,272	3,98	4,484	11,184	5,649
17	13,84	6,568	14,692	7,687	4,858	1,265	13,529	10,64	13,797	8,957
18	5,594	5,408	14,256	4,326	18,888	4,449	8,309	13,098	6,642	4,304
19	2,716	6,661	3,777	5,437	3,293	6,848	6,932	6,46	4,72	4,105
20	14,207	9,936	3,201	3,935	3,398	3,456	5,184	5,836	5,196	6,584
21	5,9	6,621	7,097	3,601	7,584	5,737	7,289	5,691	2,971	5,2
22	3,767	3,022	5,486	14,102	3,928	9,702	4,272	7,752	4,392	2,977
23	6,481	3,328	4,31	3,985	5,659	6,011	5,677	3,985	4,392	7,585
24	7,924	6,941	5,496	4,332	6,148	7,974	4,777	2,433	3,04	4,298
25	11,447	11,48	4,882	14,354	10,152	17,078	7,234	4,724	6,201	11,48
26	9,456	7,582	8,05	9,705	3,397	10,512	15,892	6,438	11,126	2,428
27	4,659	9,967	10,875	8,55	5,298	8,026	16,127	10,757	16,39	9,450
28	7,56	18,656	5,768	4,953	4,136	8,182	10,354	5,625	12,2	4,829
29	4,331	2,781	3,576	6,391	26,23	3,071	5,439	4,901	12,058	19,013
30	7,073	4,949	11,889	5,363	6,841	9,333	11,064	2,94	3,894	6,692

Dari hasil pengujian juga didapatkan 26 kali pengguna melakukan kegagalan dalam menyelesaikan CAPTCHA, sehingga prosentase pengguna gagal sebesar 7,975% sedangkan prosentase pengguna berhasil adalah 92,025%. Dari 26 kegagalan yang terjadi, terdapat 3 pola kegagalan yang sering terjadi yaitu:

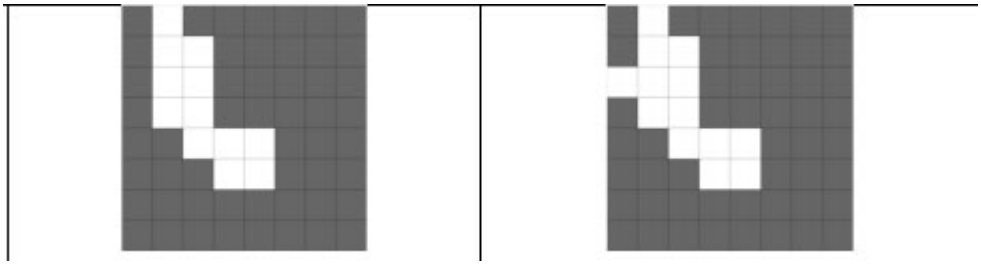
1. Pola yang mirip dengan ukuran yang berbeda
   Pengguna membentuk pola yang mirip dengan acuan tetapi terdapat perbedaan ukuran yang pengguna inputkan. Hal ini terjadi karena pola yang dibentuk oleh pengguna melebih satu kotak lebih panjang sehingga kasat mata sama dengan acuan yang diberikan oleh sistem atau pengguna membentuk pola dengan skala yang lebih besar. Contoh kegagalan ini dapat dilihat pada Gambar 11.
2. Pola yang sama dengan posisi yang berbeda
   Pengguna membentuk pola yang sama dengan acuan tetapi, pengguna membentuk acuan berada diposisi yang berbeda. Kegagalan ini terjadi karena inputan yang dibentuk pengguna berbeda 1 kotak tiap inputan sehingga menyebabkan pergeseran bentuk pola. Contoh kegagalan ini dapat dilihat pada Gambar 12.
3. Pola yang mirip dengan acuan dengan tambahan inputan
   Pengguna membentuk pola yang mirip dengan acuan tetapi pengguna menambahkan inputan yang berbeda dari acuan sehingga bentuk pola yang dibuat berbeda dengan acuan yang diberikan sistem. Kegagalan ini dapat terjadi saat mouse pengguna masih tertekan sehingga dapat menambahkan input tanpa disengaja. Contoh kegagalan ini dapat dilihat pada Gambar 13.



Gambar 11. Pola yang mirip dengan ukuran yang berbeda



Gambar 12. Pola yang sama dengan posisi yang berbeda



Gambar 13. Pola yang mirip dengan acuan dengan tambahan inputan

5. Kesimpulan Dan Saran

5.1. Kesimpulan

Kesimpulan yang dapat diperoleh dalam penelitian ini antara lain :

1. Sistem CAPTCHA dengan menggunakan permainan FLOW dapat digunakan dengan mudah oleh pengguna pada umumnya dengan tingkat rata-rata keberhasilan mencapai 92,025%, waktu penyelesaian rata-rata adalah 6,3614 detik, dan 81,67% pengguna mampu menyelesaikan kurang dari 10 detik.
2. Terdapat tiga pola kegagalan yang sering dialami oleh pengguna, yaitu pola yang mirip dengan ukuran yang berbeda, pola yang sama dengan posisi yang berbeda, dan pola yang mirip dengan acuan dengan tambahan inputan.

5.2. Saran

Untuk pengembangan kedepannya, bisa dilakukan perbaikan di bagian navigasi yang lebih bervariasi. Penelitian saat ini masih berfokus menggunakan perangkat mouse yang tentu saja memiliki tingkat usabilitas yang rendah bagi pengguna difabel.

Daftar Pustaka

Ahn, L., Blum, M., Hopper, N., & Langford, J. (2003). CAPTCHA: Using Hard AI Problems for Security. *Lecture Notes in Computer Science Advances in Cryptology — EUROCRYPT 2003, 2656,* 294-311. doi:10.1007/3-540-39200-9_18

Ahn, L., Maurer, B., McMillen, C., Abraham, D., & Blum, M. (2008). *ReCAPTCHA: Human-Based Character Recognition via Web Security Measures*. Science, Vol 321 Issue. 5895 pp. 1465-1468.

Bursztein, E., Martin, M., & Mitchell, J. (2011). Text-based CAPTCHA strengths and weaknesses. *Proceedings of the 18th ACM Conference on Computer and Communications Security - CCS '11,* 125-138.

Elson, J., Douceur, J., Howell, J., & Saul, J. (2007). Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization. *Proceedings of the 14th ACM Conference on Computer and Communications Security - CCS '07,* 366-374. doi:10.1145/1315245.1315291.

Hassanat, A. (2014). *Bypassing Captcha By Machine – A Proof for Passing The Turing Test*. European Scientific Journal Vol 10 No 15 pp 192-204.

Ho, C., Wu, C., Chen, K., & Lei, C. (2011.). *DevilTyper: A Game for CAPTCHA Usability Evaluation*. ACM Computer in Entertainment Vol 9 No 1.

Shah N.A., Banday M.T. (2009). *Image Flip CAPTCHA*. The ISC International Journal of Information Security, Vol 1, Number 2 pp 105-123.

Shirey, R. (2007). *RFC 4949 - Internet Security Glossary, Version 2*.

Stamp, M. (2011). *Information Security: Principles and Practice*. New Jersey: Wiley