

Imaged Based Authentication System dengan Reduced Difference Expansion

Muhammad Ali Sya'roni*, Yanuar Nurdiansyah**, Diksy Media Firmansyah***

Fakultas Ilmu Komputer, Universitas Jember

*muhammadalisyaroni240499@gmail.com, **yanuar_pssi@unej.ac.id, ***diksy@unej.ac.id

ABSTRACT

Authentication is an important step in a system. Text-based authentication is an authentication alternative that is currently widely used. However, text-based authentication has the disadvantage of being ineffective when users have multiple accounts. This weakness can be overcome using image-based authentication. The implementation of image-based authentication can use the Reduced Difference Expansion (RDE) steganography method. Application of image-based authentication, utilizing images as authentication media. RDE utilizes the reduced pixel difference as a place to insert credential data. Testing the image in this study, the image has an average similarity of 40 dB, indicating that the image that is inserted with credentials and that is not inserted has a high similarity. The similarity increases the security of the image from theft. The average character capacity that can be accommodated is 21,451 characters, a large enough capacity to accommodate credential data. The image is very sensitive to changes, so there is a slight change in the image, causing the image to not be used for authentication.

Keyword: Otentikasi, *Reduced Difference Expansion*

1. Pendahuluan

Otentikasi adalah aktifitas yang digunakan untuk mengidentifikasi pengguna [1]. Otentikasi sendiri terdiri dari dua tahap, tahap identifikasi dan tahap otentikasi. Tahap identifikasi adalah tahap mengidentifikasi identitas pengguna seperti *email*, *username*, dsb. Tahap otentikasi adalah tahap mencocokkan kata sandi pada *database* dengan kata sandi masukan pengguna yang terverifikasi pada tahap identifikasi [2]. Otentikasi yang paling banyak digunakan pada saat ini adalah otentikasi berbasis teks, namun, otentikasi berbasis teks memiliki kelemahan yang tidak bisa diabaikan.

Kelemahan otentikasi berbasis teks yaitu kurang efektif ketika pengguna memiliki banyak akun. Supaya keamanan akun tersebut tidak menurun, pengguna perlu membuat kredensial yang berbeda diberbagai akun, dan itu memberatkan ingatan pengguna [3]. Penelitian yang dilakukan oleh Bonneau dan Schechter, dari 94% subjek penelitiannya, memerlukan 90 kali melakukan aktifitas *log in* untuk mengingat 56 bit kata sandi [4]. Akibat dari ketidakefisienan otentikasi berbasis teks, pengguna cenderung membuat kredensial yang sama diberbagai akun [3].

Dalam sebuah penelitian yang dilakukan oleh Wash dkk menunjukkan bahwa dari 134 orang menggunakan kredensial yang sama di 9 akun yang berbeda [5]. Penelitian lain dilakukan oleh Awad dkk yang menunjukkan dari 142 orang, lebih dari 50% menggunakan kredensial yang sama diberbagai akun [6]. Penggunaan kredensial yang sama diberbagai akun yang berbeda, menurunkan keamanan dari akun itu sendiri. Pada tahun 2020, sebanyak 500.000 akun zoom terjual dalam *dark web* karena teretasnya platform lain, yang mana kredensial yang digunakan pada platform tersebut juga digunakan pada akun zoom [7].

Menurut Nitin dkk, diperlukan sebuah alternatif otentikasi untuk mengatasi kelemahan pada otentikasi berbasis teks, yaitu dengan menggunakan gambar atau citra dalam melakukan otentikasi. Otak manusia lebih mudah mengingat gambar daripada mengingat teks [8], sehingga dengan menggunakan gambar bisa meringankan beban ingatan pengguna ketika pengguna memiliki banyak akun. Menerapkan otentikasi berbasis gambar bisa dilakukan dengan menerapkan ilmu steganografi, yaitu dengan menyembunyikan kredensial kedalam sebuah citra.

Tujuan dari penelitian ini adalah memecahkan permasalahan yang telah dijelaskan pada paragraf sebelumnya dengan memanfaatkan teknik steganography. Otentikasi yang biasanya dilakukan menggunakan username dan password diubah menjadi otentikasi menggunakan citra digital yang telah diproses sedemikian rupa menggunakan teknik steganography. Dengan begitu, manfaat dari penelitian ini adalah memberikan suatu alternatif mekanisme otentikasi. Variasi mekanisme otentikasi ini diharapkan mampu meningkatkan

keamanan suatu system informasi karena semakin banyak variasi keamanan data akan mempersulit penyerang / hacker untuk mendapatkan akses ke sistem secara ilegal.

Penerapan ilmu steganografi dalam otentikasi telah dilakukan oleh beberapa peneliti. Guntoro dan Muhammad Fikri melakukan penelitian dengan menerapkan metode steganografi *Least Significant Bit* (LSB) dalam Perancangan Aplikasi *Single Sign-On* (SSO) Menggunakan Otentikasi Gambar. Eman Ibrahim Harba mengkombinasikan LSB, kriptografi AES, dan HMAC SHA-256 dalam *Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography*. Penelitian lain dilakukan oleh Irsandy Maulana Satya Viddin, Antonius Cahya P dan Diksy Media Firmansyah dengan judul penelitian Alternatif Otentikasi Menggunakan Metode Steganografi *Histogram Shifting*.

Ilmu steganografi terdiri dari berbagai metode, salah satunya metode *Difference Expansion* (DE). DE menyisipkan pesan pada selisih pasangan piksel [9]. DE memiliki berbagai kelebihan, diantaranya bersifat *reversible*, mudah digunakan, sudah banyak pengembangan yang dilakukan [10], dan jika dibandingkan dengan metode *histogram shifting*, kapasitas pada DE lebih besar [11]. Salah satu pengembangan dari metode DE ialah metode *Reduced Difference Expansion* (RDE). Metode RDE melakukan reduksi pada selisih pasangan piksel sebelum dilakukan penyisipan pesan. Reduksi yang dilakukan menyebabkan kapasitas bit pada RDE melebihi kapasitas bit pada DE, dan kualitas citra hasil penyisipan pada RDE lebih baik daripada kualitas citra hasil penyisipan menggunakan DE [12]. Berdasarkan uraian di atas, penelitian ini dilakukan untuk mengimplementasikan metode steganografi RDE sebagai alternatif otentikasi pengguna.

1.1 Steganografi

Steganografi berasal dari bahasa Yunani, yang berarti tulisan yang tersembunyi [13]. Steganografi bisa juga diartikan sebuah teknik melindungi informasi dengan cara menyembunyikan informasi tersebut kedalam sebuah media, baik berupa foto, audio, dan video [14]. Tujuan dari steganografi adalah menyembunyikan informasi sehingga tidak diketahui oleh pihak yang tidak berwenang. Tujuan tersebut berbeda dengan kriptografi, yaitu mengacak informasi sehingga tidak bisa dibaca oleh pihak yang tidak berwenang.

Menurut Lou dkk, steganografi harus memenuhi beberapa persyaratan yaitu *imperceptibility*, *robustness*, *capacity*, dan *security* [12]. Menurut Ariyus dkk, karakteristik yang harus dipenuhi dalam steganografi ialah *imperceptibility*, *fidelity*, dan *robustness* tinggi, serta *recovery* maksimum [15]. Perbedaan antara *imperceptibility* dengan *fidelity* adalah *imperceptibility* diartikan kemiripan citra secara kasat mata, sedangkan *fidelity* diartikan mutu kualitas citra.

1.2 Reduced Difference Expansion

Reduced Difference Expansion merupakan pengembangan dari metode *Difference Expansion*. Langkah langkah penyisipan dan ekstraksi pesan rahasia pada RDE hampir sama dengan penyisipan dan ekstraksi pesan rahasia pada DE. Perbedaannya terletak pada langkah reduksi pada selisih (h) sebelum disisipi pesan. Formula dari RDE itu sendiri dapat dilihat pada Persamaan 1.

$$h_{\text{reduksi}} = \begin{cases} h & \text{if } h < 2 \\ h - 2^{\lfloor \log_2 h \rfloor - 1} & \text{if } h \geq 2 \end{cases} \quad (\text{Persamaan 1})$$

Location map yang dibutuhkan pada RDE ada dua jenis, *location map* yang sama dengan DE dan *location map* yang menunjukkan selisih yang direduksi. Cara memperoleh *Location map* yang menunjukkan selisih yang direduksi dapat dilihat pada Persamaan 2.

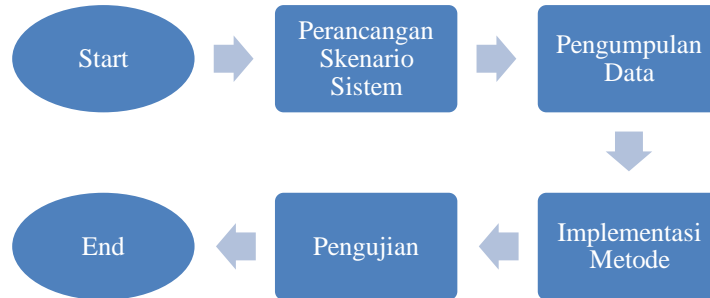
$$\text{locmap}_{\text{reduksi}} = \begin{cases} 0 & \text{if } 2^{\lfloor \log_2 h_{\text{reduksi}} \rfloor} = 2^{\lfloor \log_2 h \rfloor} \text{ or } h = h_{\text{reduksi}} \\ 1 & \text{if } 2^{\lfloor \log_2 h_{\text{reduksi}} \rfloor} \neq 2^{\lfloor \log_2 h \rfloor} \end{cases} \quad (\text{Persamaan 2})$$

Pada saat penerapan sifat *reversible* pada RDE, selisih yang direduksi perlu dikembalikan ke selisih sebelum direduksi. Cara mengembalikannya adalah dengan menggunakan Persamaan 3.

$$h = \begin{cases} h_{\text{reduksi}} + 2^{\lfloor \log_2 h_{\text{reduksi}} \rfloor - 1} & \text{jika } \text{locmap}_{\text{reduksi}} = 0 \\ h_{\text{reduksi}} + 2^{\lfloor \log_2 h_{\text{reduksi}} \rfloor} & \text{jika } \text{locmap}_{\text{reduksi}} = 1 \end{cases} \quad (\text{Persamaan 3})$$

2. Metode Penelitian

Jenis penelitian yang diterapkan adalah penelitian kuantitatif. Penelitian kuantitatif adalah penelitian yang aspek penelitiannya menggunakan pengukuran, perhitungan, rumus atau kepastian data numerik. Sedangkan tahapan-tahapan pada penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Metode Penelitian

2.1 Perancangan skenario sistem

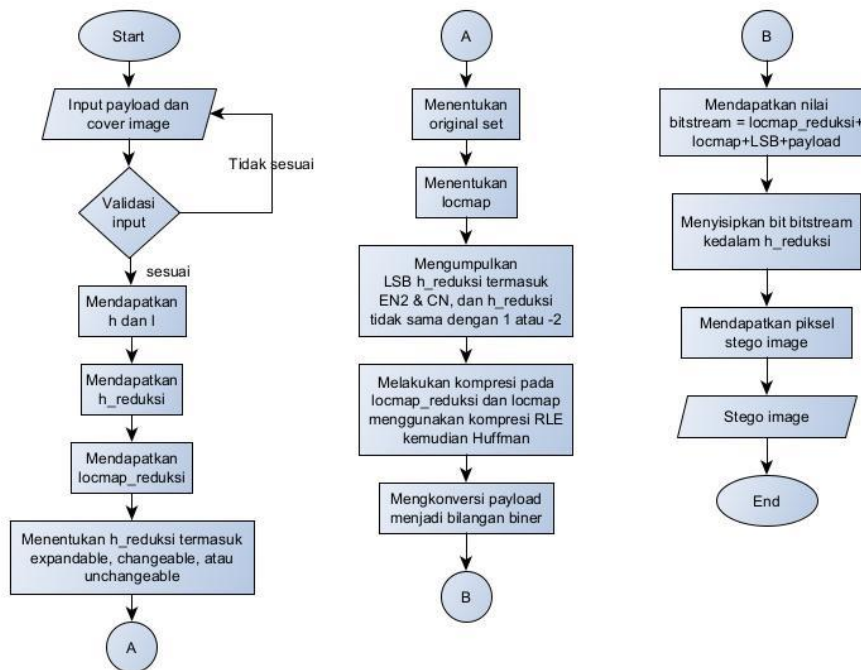
Perancangan scenario sistem bertujuan untuk terdiri dari analisis kebutuhan dan perancangan desain sistem. Tahap ini bertujuan supaya penerapan metode steganografi dalam sistem otentikasi memiliki alur yang jelas dan berjalan dengan baik.

2.2 Pengumpulan data

Pengumpulan data ialah pengumpulan citra yang akan dijadikan sebagai *stego image*. Dalam implementasi RDE, tidak semua citra bisa disisipi pesan, karena kapasitas citra dalam menampung pesan harus terbagi dengan kapasitas *location map* yang dibutuhkan. Citra yang dikumpulkan adalah citra dengan format png dan berlisensi untuk dimodifikasi.

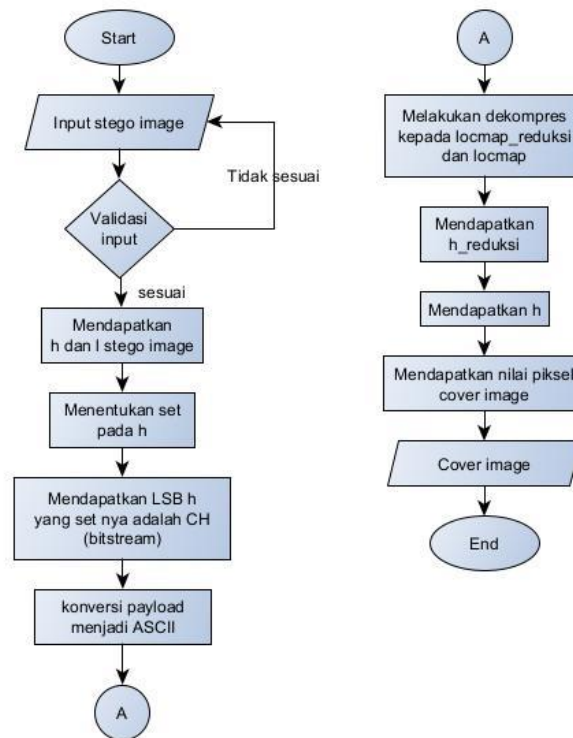
2.3 Implemetasi metode

Implementasi metode steganografi *Reduced Difference Expansion (RDE)* terdiri dari tiga tahap umum, proses penyisipan, proses ekstraksi, dan pengembalian *stego image* menjadi *cover image* (reversible). Dalam sistem otentikasi, proses pengembalian *stego image* menjadi *cover image* tidak diterapkan. Proses penyisipan pesan dilakukan ketika pengguna melakukan pendaftaran, sedangkan proses ekstraksi pesan dilakukan ketika pengguna melakukan aktifitas log in. Alur penyisipan pesan dijelaskan pada Gambar 2.



Gambar 2. Alur penyisipan pesan rahasia

Sedangkan untuk alur ekstraksi pesan dari *stego image* dijelaskan Gambar 3.



Gambar 3. Alur ekstraksi pesan rahasia

2.4 Pengujian

Pengujian dilakukan dengan dua cara, uji *fidelity*, *capacity* dan uji *robustness*. Pengujian *fidelity* dilakukan untuk mengetahui tingkat kemiripan antara *stego image* dengan *cover image* dengan menggunakan algoritma PSNR. Pengujian *capacity* bertujuan untuk mengetahui kapasitas karakter yang bisa disisipkan kedalam masing masing citra. Pengujian *capacity* akan dibandingkan dengan metode fundamental dari RDE, yaitu DE, untuk mengetahui reduksi pada selisih sudah terjadi atau tidak. Pengujian *robustness* dilakukan dengan beberapa cara, *copy paste stego image*, dikirimkan menggunakan media pengiriman, dan memanipulasi *stego image*. Hasil dari pengujian akan digunakan *log in* ke sistem otentikasi.

3. Hasil dan Pembahasan

3.1 Perancangan skenario






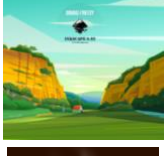
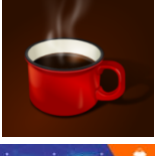


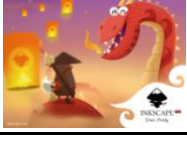
Sistem otentikasi memiliki tiga fitur utama, fitur pendaftaran, fitur masuk (*log in*) dan fitur pemulihan *stego image*. Fitur pendaftaran digunakan pengguna untuk membuat akun baru, dan setiap pembuatan *akun baru*, pengguna dapat mengunduh *stego image*. Fitur masuk digunakan pengguna ketika melakukan otentikasi, dan ketika otentikasi berhasil, pengguna memiliki hak akses ke *dashboard*. Fitur pemulihan *stego image* digunakan ketika *stego image* yang dimiliki pengguna mengalami kerusakan atau hilang.

Pada saat pendaftaran, pengguna memasukkan data diri dan memilih citra yang akan dijadikan *cover image*. Setelah pendaftaran, pengguna diarahkan ke *dashboard* dan mengunduh *stego image* untuk digunakan otentikasi kedepannya. Ketika pengguna akan melakukan aktifitas *log in*, pengguna cukup memasukkan *stego image*, kemudian sistem akan mengekstrak kredensial didalamnya untuk melakukan otentikasi. Fitur pemulihan *stego image* dapat digunakan ketika pengguna memasukkan *email*, kata sandi, dan tanggal lahir dengan benar. Kemudian, sistem akan mengirimkan *link* pemulihan *stego image* ke email pengguna.

3.2 Pencarian data

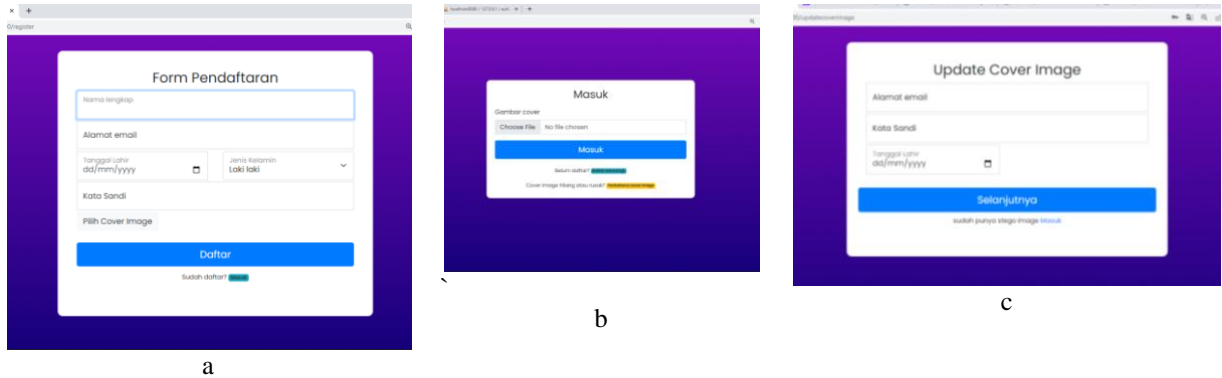
Citra dikumpulkan dari sebuah situs dengan alamat <https://inkscape.org/gallery/>. Tabel 1 merupakan citra yang bisa digunakan sebagai *cover image*.

Tabel 1. List cover image

Gambar	Nama gambar	Pencipta	Lisensi	Link
	<i>Hamburger</i>	-	Public Domain	https://inkscape.org/~theagleowl/%E2%98%85hamburger
	<i>Inkscape Funtastic</i>	Muhamad Farlly	CC-BY-SA	https://inkscape.org/~mfarly/%E2%98%85inkscape-funtastic-i-muhamad-farly
	<i>Inkscape 1.1 splash screen</i>	Fauzan Syukri	CC-BY-SA	https://inkscape.org/~ozant/%E2%98%85inkscape-11-splash-screen
	<i>Be Free</i>	Tiago Oliveira	CC-BY-SA	https://inkscape.org/id/~TiagoOHEE/%E2%98%85be-free
	<i>Travelers</i>	Олег Машков	Public Domain	https://inkscape.org/id/~VOleg/%E2%98%85travelers
	<i>Ngarai Sianok</i>	Fauzan Syukri	CC-BY-SA	https://inkscape.org/id/~ozant/%E2%98%85ngarai-sianok
	<i>Red Cup</i>	-	Public Domain	https://inkscape.org/id/~theagleowl/%E2%98%85red-cup
	<i>Next Inkscape</i>	Muhamad Farlly	CC-BY-SA	https://inkscape.org/id/~mfarly/%E2%98%85next-inkscape+1
	<i>Inkscape Bamboo</i>	Carolinacosta	CC-BY-SA	https://inkscape.org/id/~carolinacosta/%E2%98%85inkscape-bamboo
	<i>Inkscape Funtastic Dragon</i>	Muhamad Farlly	CC-BY-SA	https://inkscape.org/id/~mfarly/%E2%98%85inkscape-funtastic-dragon-i-muhamad-farly

3.3 Implementasi

Pengimplementasian metode RDE pada sistem otentikasi diterapkan di tiga fitur, fitur pendaftaran, fitur masuk (*log in*) dan fitur pembaharuan *stego image*. Fitur pendaftaran dan pembaharuan *stego image* menerapkan penyisipan kredensial, sedangkan fitur *log in* menerapkan ekstraksi kredensial dari *stego image*. Tampilan fitur fitur otentikasi seperti pada Gambar 4.



Gambar 4. Tampilan UI a) pendaftaran, b) *log in*, dan c) pemulihan *stego image*

3.4 Pengujian

Pengujian kapasitas bertujuan untuk mengetahui seberapa banyak bit yang bisa menampung pesan rahasia. Hasil pengujian kapasitas seperti pada Tabel 2.

Tabel 2. Hasil pengujian kapasitas

Gambar	Kapasitas RDE			Kapasitas DE		
	Kapasitas Total (bit)	Location map (bit)	Payload (karakter)	Kapasitas Total (bit)	Location map (bit)	Payload (karakter)
Hamburger	85.794	71.757	1.754	85.773	12.311	9.182
Inkscape Funtastic	949.584	438.422	63.895	949.293	794.014	19.409
Inkscape 1.1 Splash Screen	538.393	517.919	2.559	538.010	230.307	38.462
Be Free	570.520	246.982	40.442	570.498	102.265	58.529
Travelers	389.969	71.917	39.756	389.907	31.083	44.853
Ngarai Sianok	660.753	334.821	40.741	660.440	604.758	6.960
Red Cup	86.528	43.192	5.417	86.528	10.571	9.494
Next Inkscape	532.945	505.658	3.410	532.743	152.185	47.569
Inkscape Bamboo	204.974	181.612	2.920	204.974	73.160	16.476
Inkscape Funtastic Dragon	521.954	412.959	13.624	521.505	85.812	54.461
Rata rata	454.141	282.523	21.451	453.967	209.646	30.539

Normalnya, dengan gambar dan metode kompresi yang sama, kapasitas *payload* pada RDE lebih kecil daripada DE, karena pada RDE terdapat dua *location map*, sedangkan pada DE hanya satu *location map*. Pada gambar Inkscape *Funtastic* dan Ngarai Sianok menunjukkan sebaliknya. Kejadian tersebut disebabkan saat kompresi *location map* DE di gambar tersebut, tidak lebih kecil pada RDE.

Pada pengujian *fidelity*, menerapkan algoritma PSNR untuk mengetahui kemiripan antara *stego image* dan *cover image*. Hasil pengujian *fidelity*, dapat dilihat pada Tabel 3.

Tabel 3. Hasil pengujian kemiripan (*fidelity*)

No	Gambar	Nilai PSNR (dB)
1	Hamburger	27,46
2	Inkscape <i>Funtastic</i> karya Muhamad Farlly	35,94
3	Inkscape 1.1 <i>Splash Screen</i> by Fauzan Syukri	40,17

4	<i>Be Free</i> karya Tiago Oliveira	43,95
5	<i>Travelers</i> karya Олег Машков	49,36
6	Ngarai Sianok karya Fauzan Syukri	44,48
7	<i>Red Cup</i>	45,03
8	<i>Next</i> Inkscape karya Muhamad Farly	41,89
9	Inkscape <i>Bamboo</i> karya Carolinacosta	28,2
10	Inkscape <i>Funtastic Dragon</i> karya Muhamad Farly	43,3
Rata rata		40

Angka pengujian *fidelity* menunjukkan bahwa *cover image* dan *stego image* sangat mirip, sehingga secara kasat mata, tidak bisa dibedakan antara keduanya. Kemiripan ini menjadi penguat keamanan *stego image* dari pencurian pihak luar, karena membuat pihak luar tidak bisa membedakan antara *cover image* dan *stego image*.

Pengujian *robustness* dilakukan dengan beberapa cara, pengiriman melalui media komunikasi, salin temple (*copy paste*) dan manipulasi citra. Hasil dari pengujian *robustness* terdapat pada Tabel 4.

Tabel 4. Hasil pengujian ketahanan (*robustness*)

Mekanisme pengujian	Keberhasilan otentikasi
Dikirim melalui media komunikasi tanpa kompresi (WhatsApp document, email, dan telegram file)	Berhasil
Dikirim melalui media komunikasi dengan kompresi (WhatsApp image, instagram dan telegram photo)	Tidak berhasil
<i>Copy paste</i>	Berhasil
Manipulasi citra (<i>resize, crop, rotate, perubahan adjussment, dan penambahan filters</i>)	Tidak berhasil

RDE sangat sensitif terhadap perubahan pada *stego image*. Hal tersebut dapat dilihat dari pengujian *robustness* nomor 2 dan 4 di atas. Perubahan sedikit saja pada *stego image* menyebabkan kegagalan otentikasi. Pengujian nomor 1 dan 3 menunjukkan keberhasilan otentikasi. Hal ini terjadi karena *stego image* tidak mengalami perubahan apapun disetiap pikselnya.

4. Kesimpulan

Sistem otentikasi berbasis gambar menggunakan metode *Reduced Difference Expansion* memudahkan pengguna dalam melakukan otentikasi. Pengguna cukup memasukkan *stego image* tanpa harus mengingat password yang dia gunakan pada sistem tersebut. Ini akan sangat membantu saat pengguna memiliki banyak akun dimana pengguna tidak perlu mengingat kata sandi untuk setiap akun yang dimiliki. Hal ini akan meringankan beban ingatan pengguna **dibandingkan dengan** sistem otentikasi berbasis teks dimana pengguna harus mengingat username dan password untuk tiap akses yang dimilikinya.

Stego image yang dihasilkan sangat mirip dengan *image* yang asli (*cover image*), yaitu bernilai 39,978 dB dimana ambang batas kualitas baik bagi suatu citra digital adalah diatas 30 dB. Semakin baik kualitas (semakin mirip dengan gambar aslinya) tentu akan meningkatkan keamanan karena akan semakin tidak membuat orang lain curiga bahwa ada manipulasi terhadap citra digital tersebut. ***Stego image* juga memiliki kapasitas yang cukup baik untuk menampung kredensial, yaitu 171.617 karakter dimana sangat jarang seseorang membuat password dengan panjang di atas 100.000 karakter.**

Referensi

1. Wirdasari D. MEKANISME SISTEM OTENTIKASI PADA PROTOKOL KERBEROS VERSI 5. SAINTIKOM. 2011;; 2019-2024.
2. The Economic Times. [Online]. [cited 2021 November 13. Available from: <https://economictimes.indiatimes.com/definition/authentication>.
3. Viddin IMS, Prihandoko AC, Firmansyah D. Alternatif otentikasi menggunakan metode steganografi histogram shifting. *Jurnal Teknologi dan Sistem Komputer*. 2021 April; IX(2): 106-112.
4. Bonneau J, Schechter S. Towards Reliable Storage of 56-bit Secrets in Human Memory. In 23rd USENIX Security Symposium; 2014; San Diego: USENIX. p. 607-623.
5. Wash R, Rader E, Berman R, Wellmer Z. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) ; 2016; Denver: USENIX. p. 174-188.
6. Awad M, Al-Qudah Z, Idwan S, Jallad AH. Password security: Password behavior analysis at a small university. In 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA); 2016; Ras Al Khaimah: IEEE.
7. Tech - Redaksi CNBC Indonesia. Kacau, 530.000 Data Akun Zoom Dijual Hacker di Dark Web. [Online].; 2020 [cited 2022 August 25. Available from: <https://www.cnbcindonesia.com/tech/20200416082700-37-152270/kacau-530000-data-akun-zoom-dijual-hacker-di-dark-web>.
8. Nitin N, Chauhan DS, Sehgal VK, Sood M. Image Based Authentication System with Sign-In Seal. In World Congress on Engineering and Computer Science; 2008; San Fransisco: World Congress on Engineering and Computer Science.
9. Tian J. Reversible Data Embedding Using a Difference Expansion. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*. 2003 August; XIII(8): 890-896.
10. Rahmania LA. Pengembangan Metode Pengamanan Data Menggunakan Teknik Interpolasi antar Piksel dan Reduced Difference Expansion. *Jurnal Rekayasa Elektrika*. 2017 August; XIII(2): 87-93.
11. Narawade N, Kanphade RD. A Comparative Study of Histogram Shifting, Reversible Contrast Mapping and Difference Expansion Methods. *The IUP Journal of Information Technology*. 2015;; 60-66.
12. Lou DC, Hu MC, Liu JL. Multiple layer data hiding scheme for medical images. *Computer Standards & Interfaces*. 2009 February; XXXI(2): 329-335.
13. Akhtar N, Johri P, Khan S. Enhancing the Security and Quality of LSB based Image Steganography. In *Computational Intelligence and Communication Networks*; 2013. p. 385-390.
14. Baskara AR. STEGANOGRAFI DENGAN METODE DETEKSI FITUR DAN MAXIMIZED REDUCTION DIFFERENCE EXPANSION. ;: 1.
15. Ariyus D. Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi Yogyakarta: Andi Offset; 2008.