Available at https://jtsiskom.undip.ac.id (20 April 2021) Jurnal Teknologi dan Sistem Komputer, 9(2), 2021, 106-112
DOI:10.14710/jtsiskom.2021.13931

Alternatif otentikasi menggunakan metode steganografi histogram shifting

An authentication alternative using histogram shifting steganography method

Irsandy Maulana Satya Viddin[*1)], Antonius Cahya Prihandoko[2)], Diksy Media Firmansyah[3)]

[1)] *Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Jember*
Jl. Kalimantan No. 37, Kampus Tegalboto, Jember, Indonesia 68121

[2)] *Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Jember*
Jl. Kalimantan No. 37, Kampus Tegalboto, Jember, Indonesia 68121

[3)]*Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Jember*
Jl. Kalimantan No. 37, Kampus Tegalboto, Jember, Indonesia 68121

Cara sitasi: I. M. S. Viddin, A. C. Prihandoko, and D. M. Firmansyah, "Alternatif otentikasi menggunakan metode steganografi histogram shifting," *Jurnal Teknologi dan Sistem Komputer*, vol. 9, no. 2, pp. 106-112, 2021. doi: 10.14710/jtsiskom.2021.13931

***Abstract** – This study aims to develop an authentication alternative by applying the Histogram shifting steganography method. The media used for authentication is image media. Histogram shifting utilizes the histogram of an image to insert a secret message. The developed authentication has implemented the Histogram shifting to insert user credentials into the carrier image. Users can use the steganographic image to log into their accounts. The method extracts the credentials from the image during the login. PSNR test of the steganographic images produces an average value of 52.52 dB. The extraction capability test shows that the method can extract all test images correctly. In addition, this authentication method is also more resistant to attacks common to password authentication.*

***Keywords** – authentication; steganography; histogram shifting; user credentials*

***Abstrak** – Penelitian ini bertujuan mengembangkan alternatif otentikasi dengan menerapkan metode steganografi Histogram shifting. Media yang digunakan untuk otentikasi adalah media citra. Histogram shifting memanfaatkan histogram suatu citra untuk menyisipkan pesan rahasia. Alternatif otentikasi telah menerapkan metode Histogram shifting untuk menyisipkan kredensial pengguna ke dalam citra pembawa. Citra hasil steganografi dapat digunakan untuk masuk ke akun pengguna dengan cara mengekstrak kredensial dari citra tersebut ketika proses log in. Pengujian PSNR citra stego menghasilkan nilai rata-rata sebesar 52,52 dB. Pengujian kemampuan ekstraksi menunjukkan semua citra uji dapat diekstrak dengan tepat. Selain itu, metode otentikasi ini juga lebih tahan terhadap serangan yang umum dilakukan pada otentikasi menggunakan kata sandi.*

***Kata kunci** – otentikasi; steganografi; histogram shifting; kredensial pengguna*

I. PENDAHULUAN

Otentikasi merupkan proses yang umum pada hampir semua sistem informasi atau aplikasi saat ini. Proses tersebut bertujuan untuk mengetahui apakah seseorang atau suatu entitas memang benar memiliki hak untuk mengakses sistem atau aplikasi tersebut. Menurut [1], otentikasi dapat dikelompokkan menjadi tiga faktor, yaitu faktor pengetahuan (contohnya kata sandi berbasis teks), faktor pewarisan atau biometri (contohnya pemindai sidik jari), dan faktor kepemilikan (contohnya kartu ATM). Dibandingkan dengan tipe atau metode otentikasi lain, kata sandi berbasis teks merupakan bentuk otentikasi yang paling banyak digunakan [2].

Meski sering digunakan, metode otentikasi menggunakan kata sandi berbasis teks memiliki kelemahan tersendiri. Metode otentikasi ini mengharuskan seseorang untuk membuat kata sandi yang tidak mudah ditebak dan sekaligus mengingatnya. Apabila seseorang memiliki banyak akun digital, seperti akun media sosial, email, apliaksi jual beli online, dan *internet banking*, maka seseorang akan kesulitan untuk mengingat kata sandi setiap akun tersebut. Hal ini dapat membuat seseorang menggunakan kata sandi yang sama untuk banyak akun.

Wash dkk. [3] menunjukkan bahwa sebanyak 134 partisipan menggunakan ulang kata sandi yang sama di rata-rata 9 situs berbeda. Lebih lanjut, Florencio dan Herley [4] melakukan kajian terhadap setengah juta pengguna internet dan menunjukkan bahwa pengguna rata-rata memiliki 6,5 kata sandi yang masing-masing digunakan di 3,9 situs berbeda. Penggunaan kata sandi yang sama untuk banyak akun akan mengurangi keamanan seseorang karena apabila satu kata sandi dapat diketahui orang lain, maka akun-akun terkait dapat diserang dengan mudah. Dengan kelemahan

[*)] Penulis korespondensi (Irsandy Maulana S. Viddin)
Email: irsandymsv98@gmail.com

Submitted: 29 September 2020; Revised: 24 January 2021; Accepted: 26 February 2021; Published: 30 April 2021

metode otentikasi ini, maka dibutuhkan suatu alternatif otentikasi yang tidak membebani ingatan seseorang.

Di sisi lain, steganografi dapat digunakan untuk menyembunyikan pesan pada suatu media sedemikian hingga keberadaannya tidak diketahui. Steganografi mengubah sebuah karya secara tak terdeteksi guna menanamkan suatu pesan [5]. Media yang dapat digunakan untuk menyembunyikan suatu pesan adalah media gambar, suara, video, dan teks. Penerapan steganografi umumnya dilakukan guna menyimpan informasi rahasia dengan aman [6]–[9].

Penerapan steganografi dalam proses otentikasi telah beberapa kali dikaji sebelumnya. Fikri dan Guntoro [10] yang menerapkan steganografi dalam aplikasi *Single Sign-On* (SSO) dengan media citra. Penerapan steganografi dalam proses otentikasi yang menggunakan media suara atau audio juga dilakukan dalam [11]. Penelitian lain juga menerapkan steganografi untuk menyisipkan kata sandi ke dalam citra [12]. Ketiga penelitian tersebut menggunakan metode steganografi *Least Significant Bit* (LSB). Namun, penelitian di atas tidak menyertakan pengujian terhadap media hasil steganografi untuk mengetahui kualitasnya.

Penggunaan steganografi dalam proses otentikasi, seperti yang disebutkan sebelumnya, dapat mempermudah pengguna. Hal tersebut karena pengguna tidak harus mengingat kata sandi ataupun kredensial mereka yang telah disisipkan ke dalam media pembawa. Pengguna hanya perlu mengamankan media hasil steganografi agar tidak dicuri atau hilang. Kemudahan tersebut dapat mengatasi permasalahan terkait penggunaan kata sandi yang sama berulang kali karena pengguna susah mengingat banyak kata sandi.

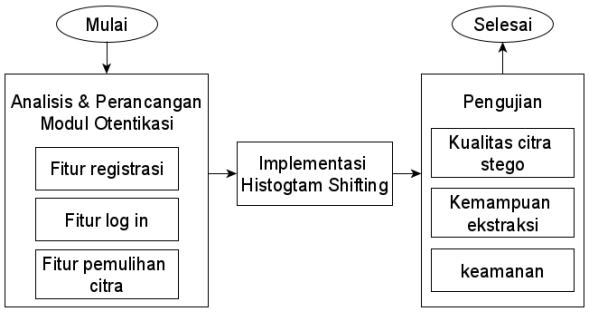
Penelitian ini bertujuan untuk menerapkan metode steganografi *Histogram Shifting* dengan media citra sebagai alternatif otentikasi. Pengujian terhadap citra hasil steganografi (citra stego), yang belum dilakukan pada penelitan terdahulu, juga dilakukan dalam penelitian ini. Pengujian lainnya yang dilakukan adalah terhadap kemampuan ekstraksi, dan pengujian keamanan modul otentikasi. Modul otentikasi ini dikembangkan berbasis web dengan menggunakan kerangka kerja pemrograman Laravel.

II. METODE PENELITIAN

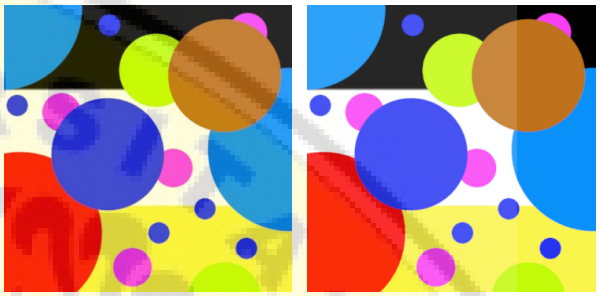
Penelitian ini dilaksanakan melalui beberapa tahapan (Gambar 1). Tahapan penelitian meliputi analisis dan perancangan modul otentikasi, implementasi metode *Histogram shifting* dalam modul otentikasi, dan pengujian. Modul otentikasi memiliki tiga fitur, yaitu registrasi, *log in*, dan pemulihan citra. Pengujian meliputi pengujian kualitas citra stego, kemampuan ekstraksi, dan keamanan.

A. Histogram shifting

Kajian ini menggunakan *Histogram shifting* sebagai metode steganografi dalam model otentikasi. Metode ini memanfaatkan histogram citra untuk menyisipkan pesan rahasia [13]. Histogram citra merepresentasikan



Gambar 1. Tahapan penelitian



(a) (b)

Gambar 2. Contoh citra asli dan hasil steganografi Histogram shifting

frekuensi atau jumlah piksel terhadap tingkat kecerahan pada suatu gambar. Melalui histogram gambar, tingkat kecerahan dengan frekuensi piksel tertinggi (*peak point*) dan frekuensi terendah (*zero point*) dapat diketahui. Nilai *peak point* dan *zero point* ini dimanfaatkan untuk menggeser tingkat kecerahan di antara kedua nilai tersebut pada histogram citra.

Gambar 2 menunjukkan citra asli sebelum disisipi pesan dan citra hasil steganografi menggunakan metode *Histogram shifting*. Pesan yang disisipkan adalah berupa teks "Steganografi merupakan ilmu yang mempelajari tentang penyembunyian pesan pada suatu media sedemikian hingga keberadaannya tidak diketahui". Kedua citra tidak menunjukkan perbedaan secara kasat mata.

B. Otentikasi menggunakan Histogram shifting

Modul otentikasi yang dikembangkan menerapkan metode *Histogram Shifting* pada fitur registrasi, *log in*, dan pemulihan citra atau kata sandi. Fitur registrasi memanfaatkan metode steganografi tersebut untuk menyisipkan kredensial terenkripsi pengguna ke dalam citra penampung. Kredensial pengguna terdiri dari email dan kata sandi. Enkripsi kredensial dilakukan menggunakan enkripsi bawaan dari kerangka kerja Laravel. Citra stego dikembalikan ke pengguna untuk masuk ke akun miliknya.

Fitur *log in* membutuhkan masukan berupa citra stego dari proses registrasi sebelumnya. Citra tersebut diekstrak untuk mendapatkan kredensial pengguna. Fitur pemulihan citra dapat mengirimkan email berisi tautan untuk memperbarui kata sandi dan citra stego pengguna. Fitur tersebut berguna ketika citra stego

pengguna rusak atau hilang. Penyisipan kredensial atau kata sandi baru ke dalam citra penampung baru dilakukan seperti pada proses registrasi.

1. Proses penyisipan

Proses penyisipan kredensial pengguna dilakukan dalam beberapa tahapan seperti dinyatakan dalam Algoritme 1. Pertama adalah menentukan panjang dan lebar citra penampung. Nilai *peak* dan *zero point* dari citra penampung diubah ke bentuk biner. Histogram digeser dengan menambah atau mengurangi 1 poin nilai tingkat kecerahan piksel yang ada di antara *peak* dan *zero point*. Penambahan dilakukan ketika nilai *peak point* lebih kecil dari *zero point*. Sebaliknya, pengurangan dilakukan ketika nilai *peak point* lebih besar dari *zero point*.

Penyisipan nilai biner *peak* dan *zero point* dilakukan ke dalam 16 piksel horizontal pertama. Penyisipan tersebut dilakukan dengan mengganti nilai biner terakhir dari suatu nilai tingkat kecerahan dengan biner *peak* dan *zero point*. Komponen warna merah atau *red* dari suatu piksel digunakan untuk penyisipan dalam penelitian ini. Langkah berikutnya, seluruh piksel citra dipindai untuk menyisipkan kredensial berbentuk biner. Penyisipan dilakukan pada piksel dengan tingkat kecerahan sama dengan *peak point*. Untuk nilai *peak point* lebih kecil zero point, jika nilai biner yang akan disisipkan adalah "1" maka nilai tingkat kecerahan piksel tersebut ditambah dengan 1 poin. Jika nilai biner adalah "0", maka nilai tingkat kecerahan tidak diubah. Untuk nilai *peak point* lebih besar dari *zero point*, maka dilakukan pengurangan 1 poin.

2. Proses ekstraksi

Proses ekstraksi kredensial dilakukan pada fitur *log in* setelah pengguna mengunggah citra stego miliknya. Proses ekstraksi *Histogram shifting* dinyatakan dalam Algoritme 2. Tahap pertama dalam proses ekstraksi adalah mendapatkan nilai biner *peak* dan *zero point* yang disisipkan pada 16 piksel horizontal pertama. Setelah didapatkan, nilai biner tersebut diubah ke bentuk desimal. Citra dipindai dengan urutan yang sama ketika proses penyisipan untuk mengekstrak nilai biner kredensial. Untuk nilai *peak point* kurang dari *zero point*, jika ditemukan piksel dengan nilai komponen warna merah sama dengan *peak point* + 1, maka nilai bit "1" diekstrak. Namun, jika nilai *peak point* lebih besar dari *zero point*, maka nilai bit "1" diekstrak ketika nilai komponen warna merah sama dengan *peak point* – 1. Jika ditemukan komponen warna merah sama dengan *peak point*, maka nilai bit "0" diekstrak. Setelah itu, nilai biner hasil ekstraksi diubah menjadi bentuk teks untuk mendapatkan kredensial terenkripsi milik pengguna.

Algoritme 1. Proses penyisipan Histogram shifting

Input: citra penampung**,** *peak point*, *zero point*, biner kredensial
Output: citra stego tersimpan ke *storage*
Funtion penyisipan (citra, peak, zero, bin_kredensial)
lebar ← jumlah piksel citra secara horizontal
tinggi ← jumlah piksel citra secara vertikal
bin_key ← nilai biner *peak* dan *zero*
for y ← 0 sampai tinggi
  for x ← 0 sampai lebar
    r ← nilai komponen warna merah piksel(x,y)
    if *peak point* < *zero point*
      if r > *peak point* && r < *zero point*
        r ← r + 1
      end if
    else
      if r < *peak point* && r > *zero point*
        r ← r - 1
      end if
    end if
    ubah nilai RGB piksel(x,y) dengan nilai r baru
  end for
end for
for x ← 0 sampai 16
  r ← nilai komponen warna merah piksel(x,0)
  r_biner ← nilai biner dari r
  ganti bit terakhir r_biner dengan bit bin_key[x]
  ubah r_biner ke bentuk desimal
  ubah nilai RGB piksel(x,y) dengan nilai r baru
end for
bin_len ← panjang bin_kredensial
jml ← 0
for y ← 0 sampai tinggi
  for x ← 0 sampai lebar
    if y == 0 && (x >= 0 && x < 16)
      continue
    end if
    if jml == bin_len
      break 2
    end if
    r ← nilai komponen warna merah piksel(x,y)
    if r == *peak point*
      if biner_kredensial[jml] == 1
        if *peak point* < *zero point*
          r ← r + 1
        else
          r ← r - 1
        end if
      end if
      ubah nilai RGB piksel(x,y) dengan r baru
      jml ← jml + 1
    end if
  end for
end for
simpan citra stego ke *storage*

C. Pengujian

Tahap pengujian terdiri dari dua bagian, yaitu pengujian citra hasil setaganografi (citra stego) dan pengujian keamanan. Pengujian citra stego dilakukan berdasarkan kriteria kualitas citra dan kemampuan ekstraksi [14].

Pengujian kualitas citra stego menggunakan metode *Peak Signal-to-Noise Ratio* (PSNR). Metode tersebut dapat mengetahui kualitas citra stego yang telah disisipi pesan rahasia dengan membandingkannya terhadap citra asli sebelum disisipi pesan rahasia dan dinyatakan dalam Persamaan 1 [15]. Parameter *PSNR* menunjukkan nilai tingkat kualitas media, sedangkan *MSE* adalah jumlah kuadrat perbedaan antara dua citra. Citra stego yang berkualitas tinggi memiliki nilai PSNR minimal 40 dB [16]. Penghitungan MSE dilakukan dengan Persamaan 2 [17], dimana *m* menunjukkan jumlah baris piksel, *n* jumlah kolom piksel, *i* indeks baris piksel, dan *j* menunjukkan indeks kolom piksel. Parameter *f* menunjukkan matriks citra asli, sedangkan *g* matriks citra stego.

$$PSNR = 10 \log \frac{255^2}{MSE} \quad (1)$$

$$MSE = \frac{1}{mn} \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} |f(i,j) - g(i,j)|^2 \quad (2)$$

Pengujian kedua adalah untuk mengetahui apakah pesan rahasia yang telah disisipkan pada citra stego dapat diungkap atau diekstrak kembali. Pengujian ini memanfaatkan fitur *log in* untuk melakukan ekstraksi pesan rahasia berupa kredensial pengguna. Jika citra stego dapat digunakan untuk masuk ke akun pengguna, maka pesan rahasia berhasil diungkap atau diekstrak.

Pengujian terakhir yang dilakukan adalah analisis beberapa teknik serangan kata sandi pada modul otentikasi yang dikembangkan. Analisis ini dilakukan untuk membandingkan keamanan modul otentikasi baru dengan otentikasi menggunakan kata sandi pada umumnya. Beberapa teknik serangan yang digunakan adalah antara lain *brute force*, *dictionary attack*, *shoulder surfing*, *key loggers*, dan *phising*.

III. HASIL DAN PEMBAHASAN

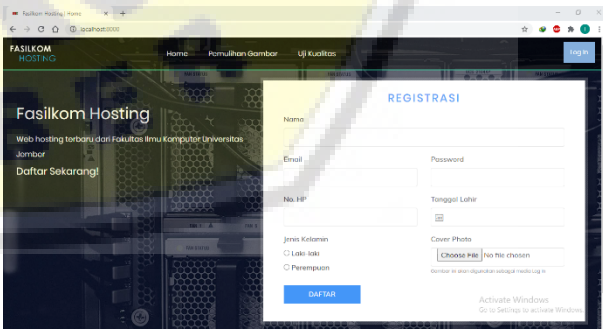
A. Modul otentikasi

Fitur registrasi digunakan untuk mendaftarkan akun pengguna baru. Fitur ini mengharuskan pengguna untuk memasukkan data diri, seperti nama, email, tanggal lahir, nomor ponsel, dan kata sandi. Selain itu, fitur registrasi juga membutuhkan masukan tambahan berupa citra atau gambar sebagai media penampung kredensial pengguna yang disisipkan. Gambar 3 menunjukkan tampilan halaman registrasi. Setelah melakukan pendaftaran, pengguna akan diarahkan ke halaman utama akun. Citra stego dapat diunduh pada halaman tersebut dan digunakan untuk masuk ke akun pengguna lain waktu.

Fitur *log in* berguna untuk masuk ke akun pengguna. Fitur *log in* pada modul otentikasi ini hanya membutuhkan masukan berupa citra stego yang diperoleh setelah melakukan registrasi. Proses ekstraksi pada fitur *log in* akan mengembalikan kredensial pengguna yang disembunyikan di dalam citra.

Algoritme 2. Proses ekstraksi Histogram shifting

Input: citra stego
Output: kredensial terenkripsi
Funtion ekstraksi (citra)
1: lebar ← jumlah piksel citra secara horizontal
2: tinggi ← jumlah piksel citra secara vertikal
3: bin_key ← “”
4: bin_kredensial ← “”
5: **for** x ← 0 sampai 16
6: r ← nilai komponen warna merah piksel(x,0)
7: r_biner ← nilai biner dari r
8: tambahkan bit terakhir r_biner ke bin_key
end for
9: *peak* dan *zero point* ← nilai desimal dari bin_key
10: **for** y ← 0 sampai tinggi
11: **for** x ← 0 sampai lebar
12: **if** y == 0 && (x >= 0 && x < 16)
continue
end if
13: r ← nilai komponen warna merah piksel(x,y)
14: **if** *peak point* < *zero point*
15: **if** r == (*peak point* + 1)
16: bin_kredensial ← bin_kredensial + “1”
else if r == *peak point*
17: bin_kredensial ← bin_kredensial + “0”
end if
else
18: **if** r == (*peak point* - 1)
19: bin_kredensial ← bin_kredensial + “1”
else if r == *peak point*
20: bin_kredensial ← bin_kredensial + “0”
end if
end if
end for
end for
21: kredensial ← bentuk teks dari nilai bin_kredensial
22: **return** kredensial



Gambar 3. Halaman registrasi

Fitur pemulihan citra ditujukan bagi pengguna yang kehilangan citra stego atau ketika citra stego miliknya mengalami kerusakan. Pengguna diharuskan membuat permintaan pemulihan dengan memasukkan alamat email dan tanggal yang digunakan ketika registrasi. Jika email dan tanggal lahir yang dimasukkan terdaftar pada basis data, maka email berisi tautan pembaruan citra dan kata sandi akan dikirimkan ke alamat email pengguna.

Setelah membuka tautan yang dikirmkan, pengguna diwajibkan memasukkan kata sandi dan citra baru. Pengguna diarahkan ke halaman utama akun miliknya untuk mengunduh citra baru yang telah dibuat. Proses penyisipan kredensial baru dilakukan seperti pada fitur registrasi.

B. Pengujian

Pengujian kualitas citra dilakukan menggunakan 10 citra uji dengan resolusi berbeda, 10 email dengan jumlah karakter yang sama, dan satu kata sandi akan disisipkan pada mesing-masing citra. Kesepuluh email tersebut berurutan dari "testUser0@mail.com" hingga "testUser9@mail.com", dengan satu kata sandi, yaitu "m9fz40]f".

Tabel 1 menunjukkan hasil perhitungan PSNR dari kesepuluh citra uji. Persamaan (1) dan (2) digunakan untuk menghitung nilai PSNR tersebut. Gambar 4 menunjukkan tiga contoh citra uji asli dan hasil steganografi. Hasil pengujian menunjukkan nilai PSNR rata-rata yang diperoleh adalah 52,52 dB. Nilai tersebut lebih tinggi dari standar nilai PSNR agar citra stego dapat dikatakan berkualitas tinggi [16]. Selain itu, nilai rata-rata tersebut lebih tinggi dari hasil pengujian pada penelitain metode *Histogram shifting* dalam [13] yang menghasilkan nilai 48 dB.

Tingginya nilai PSNR tersebut diperoleh karena penyisipan pesan rahasia hanya mengubah nilai tingkat kecerahan komponen warna piksel sebesar satu poin. Perubahan nilai yang kecil tersebut mengakibatkan nilai MSE atau perbedaan tingkat kecerahan piksel antara citra asli dan citra stego relatif rendah.

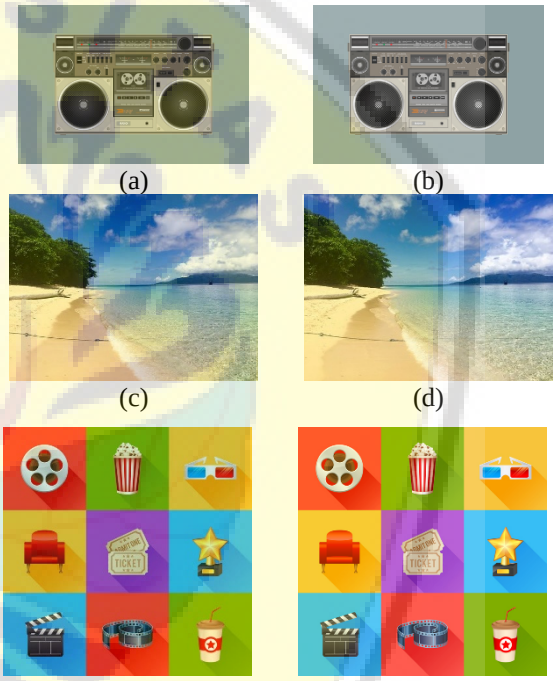
Pengujian kemampaun pengungkapan memanfaatkan 10 citra stego uji dari pengujian sebelumnya. Kesepuluh citra tersebut dicoba digunakan untuk masuk ke akun pengguna menggunakan fitur *log in*. Tabel 2 menunjukkan hasil pengujian fungsional ini. Pengujian menunjukkan bahwa semua citra stego yang diuji dapat digunakan untuk masuk ke akun pengguna. Hal ini berarti pesan rahasia, atau dalam hal ini kredensial terenkripsi, dan mampu diekstrak secara utuh tanpa kerusakan.

Keutuhan pesan rahasia menjadi penentu keberhasilan proses selanjutnya, yaitu dekripsi kredensial terenkripsi. Kredensial yang rusak akan menyebabkan proses dekripsi gagal dilakukan dan pengguna tidak dapat diotentikasi. Sebaliknya, jika kredensial mampu diekstrak secara utuh, maka proses dekripsi dapat dilakukan untuk otentikasi sistem seperti [10], [12].

Pengujian keamanan dilakukan dengan analisis teknik-teknik serangan pada modul otentikasi yang dikembangkan. Teknik serangan *brute force* dilakukan dengan mencoba semua kemungkinan kombinasi kata sandi untuk membobol akun pengguna. Teknik ini akan sulit, bahkan cenderung tidak bisa, diterapkan pada modul otentikasi yang dikembangkan karena modul otentikasi tersebut menggunakan media citra. Penyerang harus memiliki citra penampung yang sesuai untuk dapat membuat citra stego sebagai alat otentikasi. Meski sudah memiliki citra penampung, penyerang masih harus mengetahui metode steganografi untuk

Tabel 1. Hasil pengujian kualitas citra

No	Citra Stego	Resolusi (px)	MSE	PSNR (dB)
1	Citra uji 1	480 x 330	0,14	56,76
2	Citra uji 2	550 x 413	0,65	49,98
3	Citra uji 3	600 x 600	0,28	53,68
4	Citra uji 4	640 x 480	0,64	50,06
5	Citra uji 5	640 x 879	0,05	60,75
6	Citra uji 6	728 x 485	0,77	49,25
7	Citra uji 7	800 x 533	0,28	53,61
8	Citra uji 8	800 x 790	0,31	53,26
9	Citra uji 9	1280 x 720	0,87	48,73
10	Citra uji 10	1920 x 1080	0,80	49,10
Rata-rata				52,52



Gambar 4. Contoh citra uji: (a) citra asli 1, (b) citra stego 1, (c) citra asli 2, (d) citra stego 2, (e) citra asli 3, dan (f) citra stego 3

Tabel 2. Hasil pengujian kemampuan pengungkapan

No	Citra Stego	Ekstraksi	
		Berhasil	Gagal
1	Citra uji 1	V	
2	Citra uji 2	V	
3	Citra uji 3	V	
4	Citra uji 4	V	
5	Citra uji 5	V	
6	Citra uji 6	V	
7	Citra uji 7	V	
8	Citra uji 8	V	
9	Citra uji 9	V	
10	Citra uji 10	V	

menyisipkan kredensial pengguna. Selain itu, kunci dan metode kriptografi untuk mengenkripsi kredensial pengguna sebelum penyisipan juga harus diketahui.

Teknik serangan selanjutnya adalah *dictionary attack*. Teknik ini dilakukan penyerang dengan mengumpulkan kata-kata yang sering digunakan sebagai kata sandi [3], [4]. Kumpulan kata-kata ini kemudia dicoba satu per satu untuk membobol akun pengguna. Sama seperti teknik *brute force*, serangan ini sulit dan bahkan tidak bisa diterapkan pada modul otentiaksi ini. Citra yang sesuai, metode steganografi, serta kunci dan metode enkripsi harus diketahui untuk dapat menerapkan teknik ini.

Teknik serangan berikutnya adalah *shoulder surfing* yang dilakukan dengan memata-matai pengguna. Penyerang akan mencoba memperhatikan kata sandi yang diketikkan ketika pengguan akan masuk ke akunnya. Serangan ini tidak dapat diterapkan pada modul otentikasi yang dikembangkan karena pada fitur *log in* pengguna tidak perlu mengetikan apa pun. Pengguna cukup menggunggah citra stego miliknya. Meski penyerang akhirnya mengetahui citra stego pengguan dari proses memata-matai, selama penyerang tidak memiliki citra tersebut maka akun pengguna aman. Terutama bila citra yang digunakan adalah citra unik yang hanya dimiliki pengguna.

Teknik serangan *key loggers* diterapkan menggunakan program atau perangkat lunak yang dapat merekam setiap karakter yang diketikkan pada komputer yang diserang. Semua ketikan karakter yang direkam akan dikirimkan kepada penyerang yang membuat program *key loggers* tersebut. Sama seperti serangan teknik sebelumnya, teknik ini juga tidak dapat diterapkan pada modul otentikasi yang dikembangkan. Penggunaan citra stego sebagai alat otentikasi menghilangkan kebutuhan untuk mengetik kata sandi ketika pengguna akan masuk ke akunnya sehingga program seperti *key logger* tidak akan berguna pada modul otentikasi ini. Pengecualian terjadi jika program yang dibuat penyerang dapat mencuri media citra pada komputer pengguna. Jika citra stego pengguna dicuri, maka modul otentikasi yang dikembangkan dapat dibobol.

Teknik serangan terakhir adalah *phising*. Teknik ini dilakukan oleh penyerang dengan membuat situs palsu yang mirip dengan situs aslinya untuk menjebak pengguna. Ketika pengguna memasukkan kata sandi ke situs palsu tersebut, maka penyerang bisa mendapatkan kata sandi tersebut. Modul otentikasi yang dikembangkan masih rawan terhadap serangan ini. Hal tersebut karena penyerang bisa saja membuat situs palsu dengan tampilan *log in* yang mirip dengan aslinya, lalu mendapatkan citra stego pengguna. Modul otentikasi ini menggunakan citra stego sebagai alat otentikasi sehingga keamanan akun pengguna akan sangat bergantung pada citra tersebut.

IV. KESIMPULAN

Metode steganografi *Histogram shifting* berhasil diterapkan dalam modul otentikasi sebagai alternatif bagi otentiaksi berbasis kata sandi. Penerapan metode dilakukan pada fitur registrasi yang menerapkan proses penyisipan, dan fitur log in yang menerapkan proses ekstraksi. Pengujian citra stego menunjukkan kedua kriteria steganografi pada media citra berhasil dipenuhi. Pengujian keamanan menunjukkan bahwa metode otentikasi ini tahan terhadap kebanyakan serangan yang umum ditujukan pada otentikasi menggunakan kata sandi berbasis teks.

DAFTAR PUSTAKA

[1] S. W. Shah and S. S. Kanhere, “Recent trends in user authentication – A survey,” *IEEE Access*, vol. 7, no. 1, pp. 112505–112519, 2019. doi: 10.1109/ACCESS.2019.2932400

[2] S. Zulkarnain, S. Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, “A review on authentication methods adaptive biometrics view project biblio view project,” A*ustralian Journal of Basic and Applied Sciences*, vol. 7, no. 5, pp. 95–107, 2013.

[3] R. Wash, E. Rader, R. Berman, and Z. Wellmer, “Understanding password choices: how frequently entered passwords are re-used across websites,” in *Twelfth Symposium on Usable Privacy and Security*, Denver, USA, Jun. 2016, pp. 175–188.

[4] D. Florencio and C. Herley, “A large-scale study of web password habits,” in *International Conference on World Wide Web*, New York, USA, May 2007, pp. 657–666. doi: 10.1145/1242572.1242661

[5] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography, 2nd Ed*. New York: Morgan Kaufmann, 2008. doi: 10.1016/B978-012372585-1.50015-2

[6] S. Darmawan and I. Imelda, “Pengamanan dokumen menggunakan kriptografi rc4 dan steganografi eof dengan media video mp4 pada CV. Synergy Selaras,” *Jurnal Teknologi Elektro*, vol. 8, no. 2, pp. 117–122, 2017.

[7] Y. Nurdiansyah and A. L. F. Riftana, “Implementasi steganografi citra digital pemberkasan arsip menggunakan metode least significant bit,” in *Seminar Nasional Informatika dan Aplikasinya*, Bandung, Indonesia, Sep. 2017, pp. 2–7.

[8] M. K. Ridwan, W. F. Pattipeilohy, and S. Sanwani, “Aplikasi keamanan doument digital menggunakan algoritma steganografi discrete cosine transform (DCT) pada perusahan alat berat,” *Jurnal Ilmu Pengetahuan dan Teknologi Komputer*, vol. 5, no. 2, pp. 177–182, 2020. doi: 10.33480/jitk.v5i2.1033

[9] M. Syahril and H. Jaya, “Aplikasi steganografi pengamanan data nasabah di Standard Chartered Bank menggunakan metode Least Significant Bit dan RC4,” in *Seminar Nasional Sains dan Teknologi Informasi*, Medan, Indonesia, Jul. 2019, pp. 505–509.

[10] M. Fikri and G. Guntoro, “Perancangan aplikasi single sign-on (SSO) menggunakan otentikasi gambar,” *Jurnal Teknologi Informasi &*

Komunikasi Digital Zone, vol. 9, no. 1, pp. 12–21, 2018. doi: 10.31849/digitalzone.v9i1.648

[11] E. S. I. Harba, "Advanced password authentication protection by hybrid cryptography & audio steganography," *Iraqi Journal of Science*, vol. 59, no. 1c, pp. 600–606, 2018. doi: 10.24996/ijs.2018.59.1C.17

[12] S. K. Sonker, S. Kumar, A. Kumar, and P. Singh, "Image based authentication using steganography technique," *International Journal of Advanced Research in Computer Science*, vol. 4, no. 8, pp. 277–282, 2013.

[13] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–361, 2006. doi: 10.1109/TCSVT.2006.869964

[14] P. N. Andono, T. Sutojo, and M. Muljono, *Pengolahan citra digital*. Yogyakarta: Penerbit Andi, 2017.

[15] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010. doi: 10.1016/j.sigpro.2009.08.010

[16] X. Zhou, W. Gong, W. Fu, and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," in *15th International Conference on Computer and Information Science*, Okayama, Japan, Jun. 2016, pp. 1–4. doi: 10.1109/ICIS.2016.7550955

[17] D. Gupta and M. Ahmad, "An efficient method to get improved peak signal to noise ratio (PSNR), using Support Vector Machine," *International Journal of Emerging Technology and Advanced Engineering*, vol. 7, no. 9, pp. 49–53, 2017.