IMPLEMENTASI TEKNIK KRIPTOGRAFI VISUAL PADA CITRA KEABUAN DAN BERWARNA UNTUK AUTENTIKASI PENGGUNA PADA TRANSAKSI ONLINE

S. I Pella[1], Hendro F J Lami[2]

[1,2,] Program Studi Teknik Elektro, Fakultas Sains dan Teknik, Universitas Nusa Cendana
Jln.Adisucipto - Penfui, Telp. 0380-881597, Fax. 0380-881557
Email: s.i.pella@gmail.com[1]
Email: h.lami@staf.undana.ac.id[2]

Info Artikel

Histori Artikel:
Diterima Sep 03, 2021
Direvisi Okt 05, 2021
Disetujui Okt 22, 2021

ABSTRACT

Visual cryptography (VC) technique encodes an image into two or more shares that appear random in human eyes. In the decryption section, the pixels in the shared images are combined to obtain the information contained in the original image. This study applies visual cryptographic techniques to grayscale and colour images for user authentication in online transactions using the VC2,2 scheme. The server computer encodes the CAPTCHA image into two shared images that are sent to the user through different channels or applications. To authenticate himself, the user performs an XOR operation on both share images, identifies the information contained in the CAPTCHA and sends it to the server. In encryption test, histogram of the share image has a different pattern from the original image. The description test shows the decrypted image in this study visually has a better quality than the binary image has better quality than binary images.

Keywords: Visual Cryptography, Authentication, Gray Image, Colour Image

ABSTRAK

Teknik kriptografi visual (VC) mengkodekan sebuah citra kedalam citra dua atau lebih share yang terlihat acak dalam penglihatan manusia. Pada bagian dekripsi pixel pada citra share digabungkan untuk mendapatkan informasi yang ada pada citra asli. Penelitian ini menerapkan teknik visual kriptografi pada citra keabuan dan berwarna untuk autentikasi pengguna pada transaksi online menggunakan skema VC2,2. Komputer server mengkodekan citra CAPTCHA gambar kedalam dua citra share yang dikirimkan ke pengguna melalui kanal atau aplikasi yang bereda. Untuk mengautentikasi dirinya, pengguna melakukan operasi XOR terhadap kedua citra share, mengidentifikasi informasi yang terkandung dalam CAPTCHA dan mengirimkannya ke server. Pengujian hasil enkripsi menunjukkan histogram citra share mempunyai pola yang berbeda dengan citra asli. Pengujian deskripsi menunjukkan citra hasil dekripsi pada penelitian ini secara visual mempunyai kualitas yang lebih baik dari citra biner.

Kata Kunci: Visual Kriptografi, Autentikasi, Citra Keabuan, Citra Berwarna

Penulis Korespondensi:
S. I Pella
Program Studi Teknik Elektro Fakultas Sains dan Teknik,
Universitas Nusa Cendana,
Jl. Adisucipto Penfui - Kupang.
Email: s.i.pella@gmail.com

3.1.PENDAHULUAN

Kriptografi visual merupakan teknik kriptografi untuk enkripsi citra yang menggunakan penglihatan manusia untuk proses dekripsinya. Citra asli dienkripsikan kedalam beberapa citra baru (*share*) melalui penambahan noise dengan pola tertentu sehingga setiap *share* terlihat acak. Secara tradisional, proses dekripsi pada kriptografi visual dilakukan dengan mencetak

citra *share* pada kertas transparan dan menumpuk citra *share*[1]. Pada perkembangannya, proses dekripsi bisa dilakukan dengan operasi logika XOR atau AND menggunakan program komputer. Model awal kriptografi visual menggunakan citra biner (hitam putih) [1]. Pengembangan algoritma visual kriptografi, memungkinkan enkripsi untuk citra keabuan[2] dan warna[3, 4].

Penerapan kriptografi visual untuk telah dilakukan pada berbagai bidang seperti *watermarking*, sistem anti-phising, pengamanan citra resi digital, autentikasi pengguna aplikasi online, dan keamanan citra [5-8].

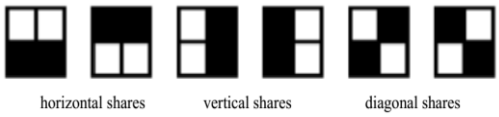
Penelitian pada [8, 9] membahas penggunaan kriptografi visual untuk mengamankan transaksi belanja online dengan cara mengenkripsi CAPTCHA dan QR code menggunakan model kriptografi visual citra biner. Model ini bekerja dengan baik pada citra yang hanya mengandung text, tetapi menghasilkan dekripsi dengan kualitas rendah untuk citra yang mengandung obyek selain teks[10]. Pada praktiknya CAPTCHA dapat berbentuk teks maupun objek lainnya.

Penelitian ini membahas implementasi visual kriptografi pada citra keabuan dan berwarna untuk captcha yang mengandung gambar. Susunan artikel adalah sebagai berikut. Pada bagian 2, dibahas metode penelitian meliputi model kriptografi citra biner, model kriptografi citra keabuan dan warna, dan model autentikasi online dengan kriptografi visual. Pada bagian 3 dibahas hasil dan pengujian sistem yang dibangun. Bagian 4 berisikan kesimpulan dari penelitian ini.

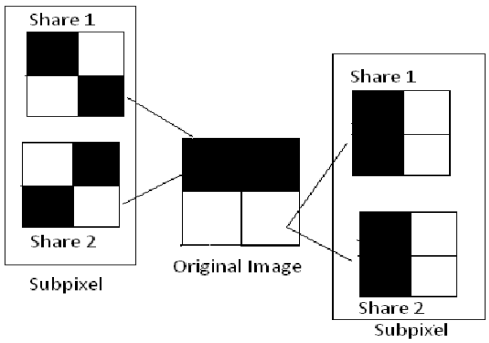
3.2.METODE PENELITIAN

2.1. Teknik Kriptografi Visual pada Citra Biner

Pada model dasar kriptografi visual [1], sebuah citra rahasia di enkripsikan kedalam n buah citra share, dimana apabila sekelompok tertentu citra share ditumpuk akan menampilkan informasi yang terdapat pada citra asli. Skema enkripsi pada kroptografi visual dikodekan dengan VCn,k, dimana n adalah jumlah citra share yang dibangun dan k adalah jumlah citra share yang dibutuhkan untuk menampilkan informasi yang terdapat pada citra rahasia. Pada model enkripsi VC 2,2 , sebuah pixel pada citra asli dienkripsi kedalam 4 sub-pixel pada citra *share*. Kombinasi sub-pixel citra share pada model VC 2,2 dapat dilihat pada gambar 1(a). Pixel hitam dienkripsikan menggunakan 2 kombinasi sub-pixel yang berlawanan pada citra share dan pixel putih dienkripsikan menggunakan 2 kombinasi sub-pixel yang sama, seperti ditunjukkan pada gambar 1(b).



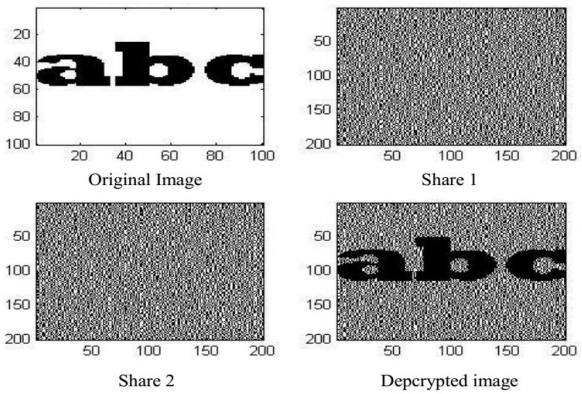
(a) Kombinasi sub Pixel VC2,2 [1]



(b) Enkripsi Sub Pixel VC2,2 [10]

Gambar 1 Sub-Pixel Citra Share Pada Skema VC2,2

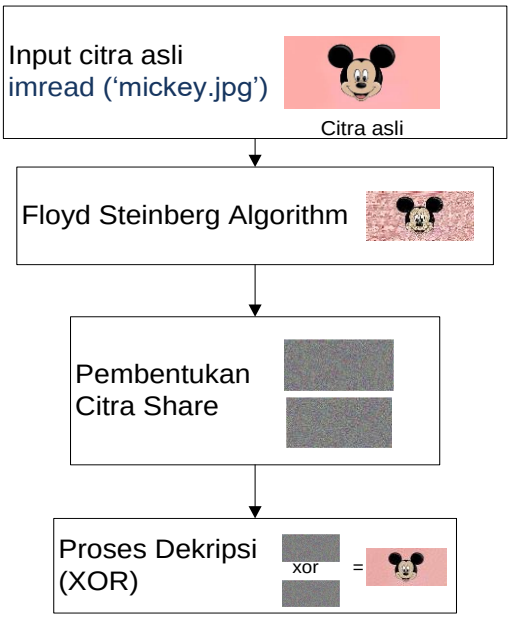
Pada proses dekripsi, pixel hitam akan terlihat sebagai warna hitam oleh mata manusia, sedangkan pixel putih akan terlihat seperti warna abu-abu, seperti terlihat pada gambar 2.



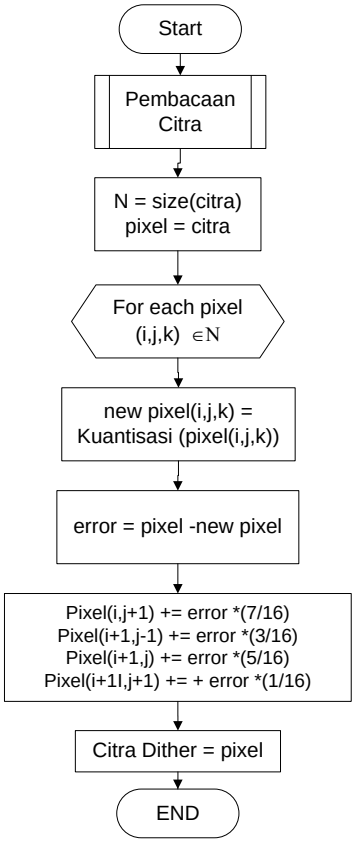
Gambar 2 Hasil Dekripsi VC2,2 pada citra biner [10]

2.2. Model Kriptografi Visual pada Citra Keabuan dan Warna

Blok diagram implemetasi kriptografi visual citra keabuan dan warna pada penelitian terlihat pada Gambar 3. Citra asli diproses menggunakan algoritma dithering Floyd-Steinberg menjadi citra halftone dengan kualitas yang lebih rendah. Citra halftone kemudian dienkripsikan menggunakan modifikasi algoritma pada bagian 2.1 menjadi dua citra share yang tampak acak di mata manusia. Pada bagian dekripsi, proses penumpukan 2 citra share (operasi xor pada program) menampilkan informasi pada citra asli.



Gambar 3 Blok Diagram Kriptografi Visual Warna VC2,2



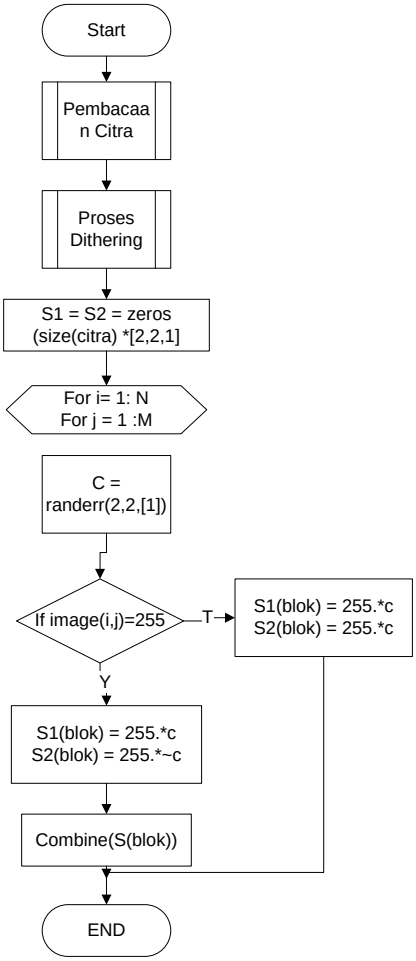
Gambar 4 Flowchart Proses Dithering dengan Algoritma Floyd-Steinberg

A. Algoritma Dithering Floyd-Steinberg

Proses dithering adalah proses penambahan derau pada data digital dengan menambahkan kesalahan kuantisasi secara acak. Proses ini digunakan pada citra, audio maupun video. Algoritma Floyd-Steinberg menggunakan teknik difusi kesalahan, dimana kesalahan kuantisasi sebuah pixel didistribusikan kepada pixel-pixel tetangganya.

Implementasi proses dithering dengan algoritma Floyd-steinberg dapat dilihat pada flowchart Gambar 4.

Pixel(i,j) pada citra asli dikuantisasi ke level terdekat. Kemudian error kuantisasi dihitung menggunakan selisih nila pixel pada citra asli dengan pixel baru hasil kuantisasi. Nilai error ini kemudian disebarkan ke pixel tetangga. Proses ini diulang untuk setiap pixel pada gambar asli. Perbedaan citra keabuan dan citra warna pada implementasi ini adalah pada koefisien k. Pada citra keabuan hanya terdapat 1 kanal, maka nilai k =1. Pada citra warna mode RGB, dengan kanal R,G dan B, nilai k $\in$ {1,2,3).



Gambar 5 Flowchart Pembangkitan Citra *Share*

B. Proses Pembangkitan Citra Share

Proses pembangkitan citra share merupakan modifikasi dari model algoritma dasar kriptografi visual pada bagian 2.1. Untuk setiap pixel pada citra dithered dienkripsi ke dalam 4 sub-pixel pada citra share. Pixel dengan nilai 255 pada setiap

kanal di enkripsi seperti pixel berwarna putih pada citra biner. Pixel bernilai 0 pada setiap kanal dienkripsi seperti pixel hitam pada gambar biner. Flowchart proses pembangkitan citra share dapat dilihat pada Gambar 5.

2.3. Sistem Autentikasi Transaksi Online Menggunakan Visual Kriptografi

Sistem Authentikasi yang dirancang pada penelitian ini mengikuti blok diagram di Gambar 6. Pada saat seorang pengguna melakukan permintaan autentikasi ke server, server membangkitkan sebuah informasi secara acak (m) kemudian menyisipkan informasi tersebut dalam bentuk captha. Server kemudian melakukan enkripsi pada citra captcha menggunakan skema VC2,2, menghasilkan dua citra *share* yang terlihat acak. Kedua citra *share* dikirimkan ke pengguna melalui dua kanal atau aplikasi yang berbeda. Apabila seorang *intruder* berhasil membobol sebuah kanal, intruder tersebut hanya mendapatkan sebuah share yang terlihat acak, dan tidak mungkin mendapatkan informasi yang terkandung dalam Captcha.

Pengguna yang sah akan mendapatkan kedua *share* yang dikirim server dan melakukan proses XOR untuk mendapatkan citra captcha. Pengguna lalu mengidentifikasi informasi yang terdapat pada captcha (m') dan mengirimkan informasi tersebut ke server. Apabila nilai m sama dengan nilai (m'), maka proses autentikasi diterima, pada keadaan sebaliknya proses autentikasi ditolak

3.3.HASIL DAN PEMBAHASAN

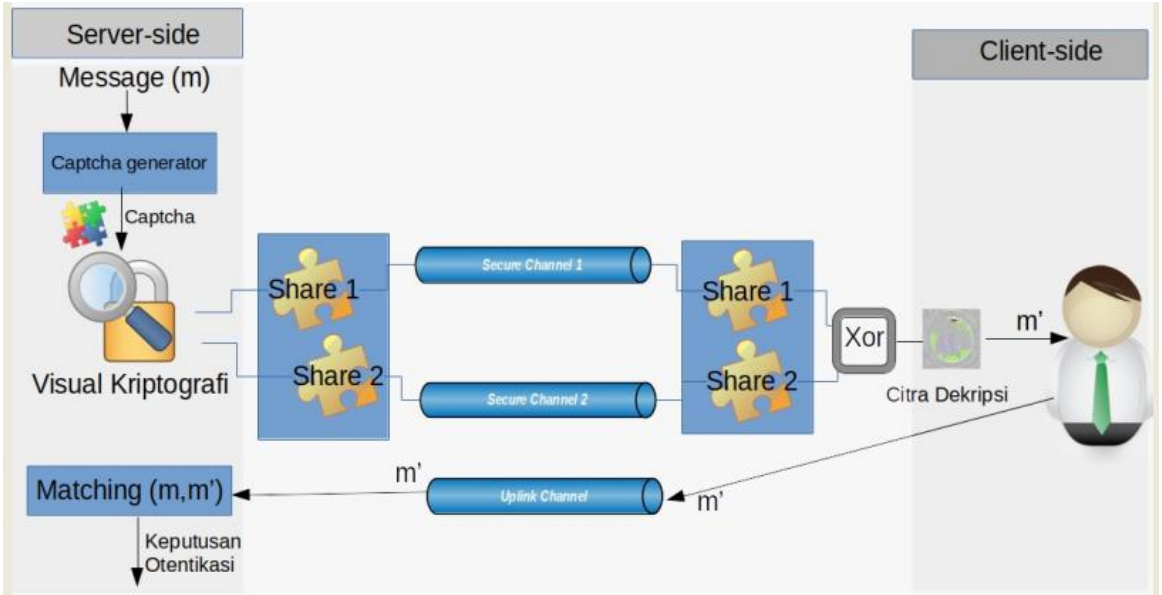
3.1. Proses Dithering Citra Asli dengan Algoritma Floyd-Steinberg

Proses dithering pada penelitian ini mengubah 256 warna pada citra asli menjadi 8 warna dasar pada citra *halftone* seperti terlihat pada Tabel 1.

Tabel 1 Warna Dasar pada Proses Dithering

[R, G, B]	Warna
[0,0,0]	Hitam
[0,0,255]	Biru
[0,255,0]	Lime
[0,255,255]	Cyan
[255,0,0]	Merah
[255,0,255]	Magenta
[255,255,0]	Kuning
[255,255,255]	Putih

Hasil proses dithering citra grayscale dan warna dapat dapat dilihat pada Gambar 7. Setiap pixel di citra asli dikuantisasi ulang , kemudian hasil derau kuantisasinya disebarkan ke pixel-pixel tetangga.



Gambar 6 Blok Diagram Otetikasi Pengguna dengan Kriptografi Visual


(a) Citra Asli Keabuan

(b) Citra Dithered Keabuan

(c) Citra Asli Warna

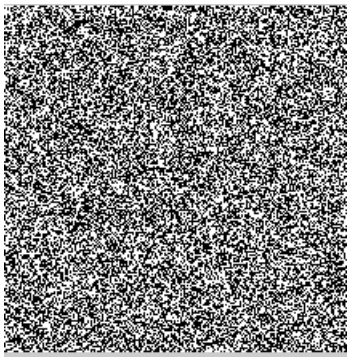
(d) Citra Warna Dithered

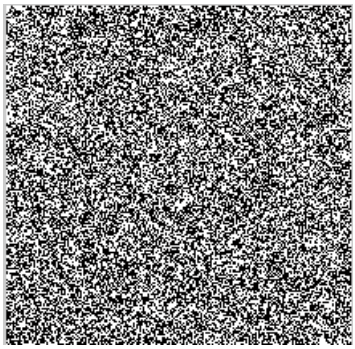
Gambar 7 Hasil *Dithering* pada Citra Keabuan dan Berwarna

3.2. Enkripsi dengan VC2,2

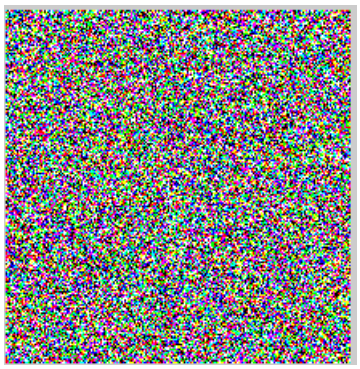
Hasil pengujian enkripsi d pada citra keabuan terlihat pada gambar 8. Citra *share* 1 dan citra *share* 2 terlihat acak dan tidak menampilkan karakteristik citra asli.

Hasil pengujian enkripsi pada citra warna terlihat pada gambar 9. Seperti pada citra keabuan, citra *share* pada citra warna tidak menampilkan karakteristik gambar asli.


(a) Citra Share 1


(b) Citra Share 2

Gambar 8 Enkripsi Citra Keabuan


(a) Citra Share 1


(b) Citra Share 2

Gambar 9 Enkripsi Pada Citra Warna

3.3. Analisa Kualitas Citra

A. Perbandingan Visual Kualitas Citra Dekripsi

Perbandingan visual kualitas citra dekripsi dapat terlihat pada Gambar 10. Citra hasil dekripsi pada model kriptografi visual biner seperti yang dideskripsikan di [10] dan [8] terlihat pada

Gambar 10(a). Citra hasil dekripsi menunjukkan penurunan kualitas yang cukup jauh terhadap citra

(a) (b) (c)

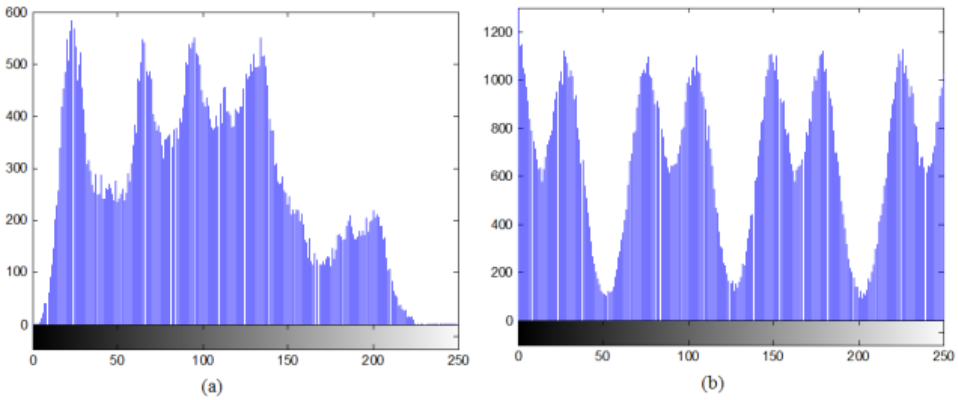
Gambar 10 Perbandingan Visual Citra Hasil Dekripsi

asli dan hampir tidak dapat dikenali oleh mata. Citra hasil dekripsi dengan model kriptografi visual keabuan dan warna terlihat pada Gambar 10(b) dan 10(c). Pada citra hasil dekripsi terlihat penurunan kualitas terhadap citra asli. Hal ini disebabkan karena proses dithering menghasilkan derau kuantisasi dan proses enkripsi menambahkan derau acak pada citra *share*. Meskipun demikian, secara visual, objek lebih mudah dikenali daripada pada enkripsi menggunakan model biner.

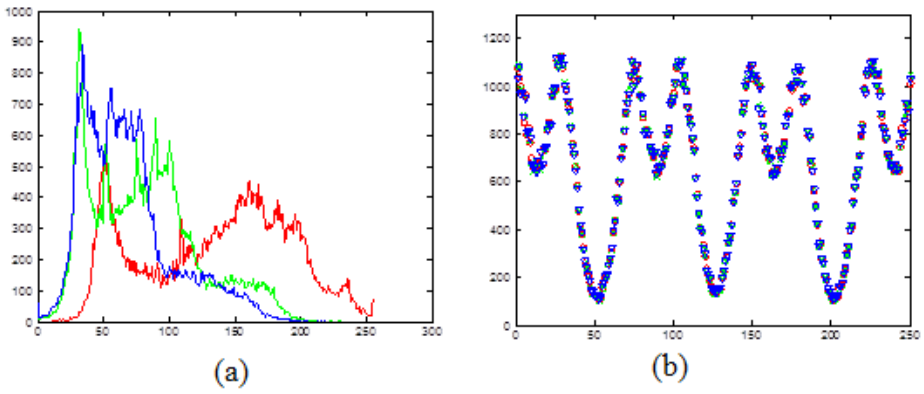
B. Analisa Kualitas Citra Enkripsi

Untuk menjamin keamanan, citra *share* harus terlihat acak di mata manusia dan tidak menggambarkan pola pada citra asli. Pada pengujian kualitas citra enkripsi, digunakan histogram untuk membandingkan frekuensi nilai intensity setiap pixel pada gambar asli dan citra hasil enkripsi.

Seperti histogram citra pada umumnya, sumbu x menunjukkan nilai dari setiap pixel dan sumbu y menunjukkan frekuensi nilai tersebut pada citra. Histogram citra keabuan terdapat 1 kanal menunjukkan intensitas derajat keabuan dari 0 (pixel hitam) sampai 255 (pixel putih). Untuk citra berwarna, histogram terdiri dari 3 kanal R,G dan B, dengan nilai 0 sampai 255.



Gambar 11 Histogram Citra Keabuan



Gambar 12 Histogram Citra Warna

Gambar 10 dan 11 menampilkan histogram citra keabuan dan citra warna. Bagian (a) pada setiap gambar menunjukkan histogram citra asli dan bagian (b) citra hasil enkripsi. Dapat dilihat pada grafik bahwa histogram citra enkripsi memiliki karakteristik yang berbeda dengan citra asli, menunjukkan bahwa citra asli tidak tergambar pada citra enkripsi. Selain itu juga terlihat bahwa citra enkripsi mempunyai penyebaran frekuensi intensitas yang cenderung seragam mengakibatkan citra enkripsi terlihat acak oleh mata. Pada Citra enkripsi warna, terlihat setiap warna (R,G,B) mempunyai distribusi frekuensi intensitas yang sama, menunjukkan pada bahwa citra share, warna R,G dan B mempunyai distribusi yang sama.

4. KESIMPULAN

Artikel ini telah membahas implementasi kriptografi visual pada citra keabuan dan citra warna untuk autentikasi pengguna pada transaksi online. Proses enkripsi meliputi proses dithering dan proses pembangkitan citra *share*. Proses dekripsi menggunakan operasi XOR. Hasil pengujian menunjukkan, walaupun mengalami penurunan kualitas dibandingkan citra asli, citra hasil dekripsi pada penelitian ini lebih baik daripada sistem yang menggunakan citra biner (Gambar 10). Hasil histogram dari citra share dan citra asli menunjukkan kedua citra ini mempunyai distribusi intensitas yang sangat berbeda. Selain itu distribusi frekuensi intensitas pixel pada citra share yang cenderung seram menunjukkan bahwa citra *share* terlihat acak pada penglihatan manusia.

DAFTAR PUSTAKA

[1] M. Naor and A. Shamir, "Visual cryptography," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1994, pp. 1-12.

[2] E. Myodo, K. Takagi, S. Miyaji, and Y. Takishima, "Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique," in *2007 IEEE International Conference on Multimedia and Expo*, 2007, pp. 2114-2117.

[3] K. Shankar and P. Eswaran, "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography," *China Communications*, vol. 14, pp. 118-130, 2017.

[4] M. Karolin and D. T. Meyyapan, "RGB based secret sharing scheme in color visual cryptography," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, 2015.

[5] H. Kaur and P. Khanna, "Biometric template protection using cancelable biometrics and visual cryptography techniques," *Multimedia Tools and Applications*, vol. 75, pp. 16333-16361, 2016.

[6] H. Abdolrahimpour and E. Shahab, "A short survey of visual cryptography and secret image sharing techniques and applications," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 4, pp. 58-62, 2017.

[7] G. S. Mary and S. M. Kumar, "Secure grayscale image communication using significant visual cryptography scheme in real time applications," *Multimedia Tools and Applications,* vol. 79, pp. 10363-10382, 2020.

[8] T. Yuniati and I. Kresna A, "Metode Pembayaran Elektronik yang Aman pada Online Shopping Berbasis Kriptografi Visual," *Rekayasa Sistem dan Teknologi Informasi (RESTI),* vol. 4, pp. 319-328, 2020.

[9] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography," in *2014 IEEE Students' Conference on Electrical, Electronics and Computer Science*, 2014, pp. 1-5.

[10] S. I. Pella and M. Pella, "Implementation of Visual Cryptography Techique on Square BW Secret Image," *Jurnal Media Elektro,* vol. 1, pp. 7-12, 2012.