Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13727
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Terbit : 05 Juni 2024

Perbandingan Skema Kriptografi Visual Analisis Kinerja PSNR, NCC, dan MSE

[1]Sugianto, [2] Jimmy, [3]Tiarma Simanihuruk
[1, 2, 3]Universitas IBBI

[1]sugiantoshi@gmail.com, [2]jimmy_khuang@hotmail.co.id, [3]tiarma.simanihuruk@gmail.com

ABSTRAK

Kriptografi visual adalah teknik yang menyediakan keamanan untuk data multimedia dengan mengenkripsi gambar rahasia menjadi beberapa bagian. Gambar rahasia hanya dapat diungkapkan ketika semua bagian digabungkan. Keuntungan utama dari kriptografi visual adalah bahwa dekripsinya dapat dilakukan oleh sistem visual manusia tanpa bantuan komputer. Penelitian ini membandingkan kriptografi visual tradisional, kriptografi visual diperluas, dan kriptografi visual berwarna berdasarkan PSNR, NCC, dan MSE. Hasil analisis menunjukkan bahwa kinerja kriptografi visual berwarna lebih baik dibandingkan dengan kriptografi visual tradisional dan diperluas.

Kata Kunci: Kriptografi Visual, Kriptografi Visual Diperluas, Kriptografi Visual Berwarna, PSNR, NCC, MSE

PENDAHULUAN

Era digital telah mengubah cara kita berkomunikasi dan bertukar informasi. Data multimedia, seperti gambar dan video, kini menjadi bagian penting dari komunikasi sehari-hari, terutama dengan meningkatnya penggunaan platform media sosial, aplikasi pesan instan, dan layanan berbagi file. Namun, kemudahan dalam pertukaran data ini juga membawa tantangan signifikan terkait keamanan dan privasi data. Ancaman seperti peretasan, pencurian data, dan penyadapan telah menjadi masalah umum yang perlu diatasi.

Kriptografi adalah salah satu cara utama untuk melindungi data dari akses yang tidak sah. Sementara metode kriptografi tradisional, seperti AES (Advanced Encryption Standard) dan RSA (Rivest-Shamir-Adleman), efektif untuk teks dan data numerik, mereka kurang optimal untuk melindungi data multimedia. Hal ini disebabkan oleh kebutuhan komputasi yang tinggi dan ketergantungan pada perangkat keras dan perangkat lunak khusus untuk dekripsi.

Visual cryptography (VC) diperkenalkan oleh Naor dan Shamir pada tahun 1994 sebagai solusi untuk mengatasi masalah ini. VC adalah teknik kriptografi yang memungkinkan data visual dienkripsi sedemikian rupa sehingga dekripsinya dapat dilakukan hanya dengan menggunakan penglihatan manusia, tanpa memerlukan komputer. Teknik ini bekerja dengan membagi gambar rahasia menjadi beberapa bagian (share) yang terlihat seperti pola acak. Ketika bagian-bagian ini digabungkan (ditumpuk), gambar asli akan muncul tanpa perlu komputasi tambahan.

Skema VC tradisional menggunakan gambar biner hitam dan putih untuk representasi data visual. Meskipun efektif, skema ini memiliki beberapa kelemahan, seperti kehilangan resolusi dan kontras gambar. Untuk mengatasi masalah ini, skema VC diperluas (Extended Visual Cryptography atau EVC) dan skema VC berwarna (Color Visual Cryptography atau CVC) telah dikembangkan. EVC memperkenalkan konsep bagian yang bermakna, di mana setiap bagian menyerupai gambar

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13727
e-ISSN : 2797-3298
p-ISSN : 2089-9424

yang dapat dikenali, sehingga mengurangi kecurigaan bahwa gambar tersebut telah dienkripsi. CVC, di sisi lain, memungkinkan penggunaan gambar berwarna, meningkatkan kualitas visual dan mengurangi kecurigaan.

Penelitian ini bertujuan untuk membandingkan kinerja tiga skema kriptografi visual utama - VC tradisional, EVC, dan CVC - berdasarkan tiga parameter utama: Peak Signal to Noise Ratio (PSNR), Normalized Correlation Coefficient (NCC), dan Mean Square Error (MSE). PSNR mengukur kualitas gambar yang dienkripsi dibandingkan dengan gambar aslinya; NCC mengevaluasi korelasi antara gambar asli dan gambar yang dipulihkan; dan MSE mengukur rata-rata kesalahan kuadrat antara gambar asli dan gambar yang dipulihkan. Dengan menganalisis ketiga parameter ini, kami dapat menentukan skema kriptografi visual mana yang menawarkan kinerja terbaik dalam hal kualitas gambar dan keamanan.

Penelitian ini diorganisir sebagai berikut: Bagian Metode menjelaskan prosedur dan teknik yang digunakan dalam masing-masing skema kriptografi visual. Bagian Analisis memberikan tinjauan mendalam tentang hasil pengujian dan perbandingan antara skema. Bagian Kesimpulan merangkum temuan utama dari penelitian ini dan menawarkan rekomendasi untuk pekerjaan di masa depan dalam bidang kriptografi visual.

METODE

1. Kriptografi Visual Tradisional

Kriptografi visual tradisional mengenkripsi gambar rahasia menjadi beberapa bagian yang dapat diungkapkan ketika semua bagian digabungkan. Skema ini menggunakan piksel hitam dan putih untuk merepresentasikan gambar biner. Gambar rahasia dipecah menjadi dua atau lebih bagian (shares), di mana setiap bagian terlihat seperti pola acak yang tidak bermakna jika dilihat secara terpisah. Namun, ketika bagian-bagian ini ditumpuk, gambar asli akan muncul tanpa perlu komputasi tambahan.

Langkah-langkah dalam Kriptografi Visual Tradisional:

1) Pemisahan Gambar:
   a. Gambar asli dipecah menjadi beberapa bagian.
   b. Setiap bagian hanya berisi informasi parsial dari gambar asli.

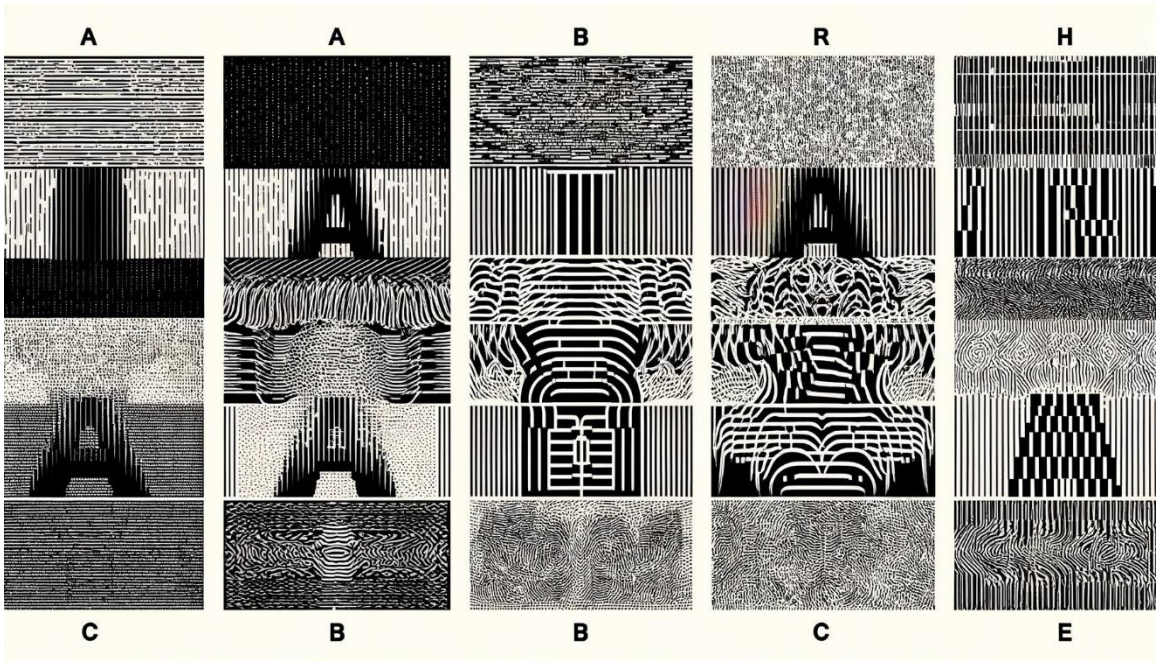
2) Proses Pembuatan Bagian (Shares):
   a. Setiap piksel pada gambar asli dikodekan menjadi beberapa piksel pada masing-masing bagian.
   b. Sebagai contoh, sebuah piksel putih pada gambar asli dapat dipecah menjadi dua piksel putih pada dua bagian berbeda, atau sebuah piksel hitam dapat dipecah menjadi dua piksel dengan pola hitam-putih.

3) Rekonstruksi Gambar:
   a. Gambar asli dapat direkonstruksi dengan menumpuk semua bagian yang dihasilkan.
   b. Proses penumpukan dilakukan secara visual tanpa memerlukan komputasi.

Tabel 1: Pola Piksel untuk Kriptografi Visual Tradisional

Piksel Asli	Nilai Piksel	Bagian 1	Bagian 2	Bagian 1 + Bagian 2
Putih	0	1	0	1
Hitam	1	0	1	1
Putih	0	1	1	0
Hitam	1	0	0	1

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13727
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 1: Contoh Bagian Kriptografi Visual Tradisional

(a) Pola Garis Horizontal
(b) Pola Garis Vertikal
(c) Pola Garis Diagonal

Setiap panel menampilkan pola yang tampak acak. Ketika digabungkan, panel-panel ini mengungkapkan gambar asli, dalam hal ini huruf "A".

2. Kriptografi Visual Diperluas (Extended Visual Cryptography)

Kriptografi visual diperluas menciptakan bagian yang bermakna bagi siapa saja yang melihatnya, sehingga mengurangi kecurigaan bahwa telah terjadi enkripsi. Setiap bagian terlihat seperti gambar yang dapat dikenali (misalnya, gambar hewan atau objek sehari-hari). Setelah bagian-bagian ini digabungkan, informasi rahasia diungkapkan.

Langkah-langkah dalam Kriptografi Visual Diperluas:

1) **Pembuatan Bagian yang Bermakna:**

   a. Setiap bagian dibuat sedemikian rupa sehingga terlihat seperti gambar yang dapat dikenali.
   b. Pola piksel pada setiap bagian tidak acak, tetapi diatur untuk membentuk gambar tertentu.

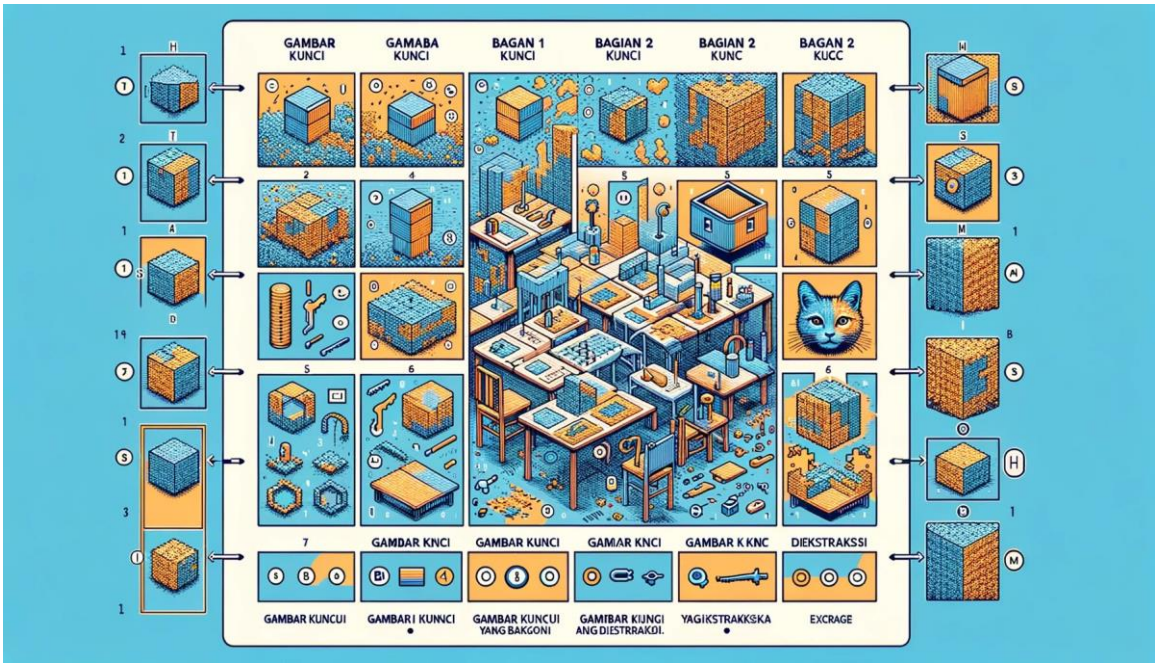
2) **Proses Pembuatan Bagian:**

   a. Gambar asli dikodekan menjadi beberapa bagian dengan pola piksel yang bermakna.
   b. Setiap bagian tetap terlihat seperti gambar acak, tetapi ketika digabungkan, gambar asli akan muncul.

3) **Rekonstruksi Gambar:**

   a. Gambar asli diungkapkan dengan menumpuk semua bagian yang dihasilkan.
   b. Proses penumpukan dilakukan secara visual tanpa memerlukan komputasi.

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13727
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 2: Contoh Gambar Kunci dalam EVC

a) Gambar Kunci
b) Bagian 1
c) Bagian 2
d) Gambar Kunci yang Diekstraksi

3. Kriptografi Visual Berwarna (Color Visual Cryptography)

Kriptografi visual berwarna menggunakan gambar berwarna untuk menyembunyikan rahasia, yang dapat dikodekan dan diungkapkan tanpa menggunakan komputer. Teknik ini sering menggunakan metode halftoning untuk menghasilkan bagian dengan kualitas visual yang signifikan.

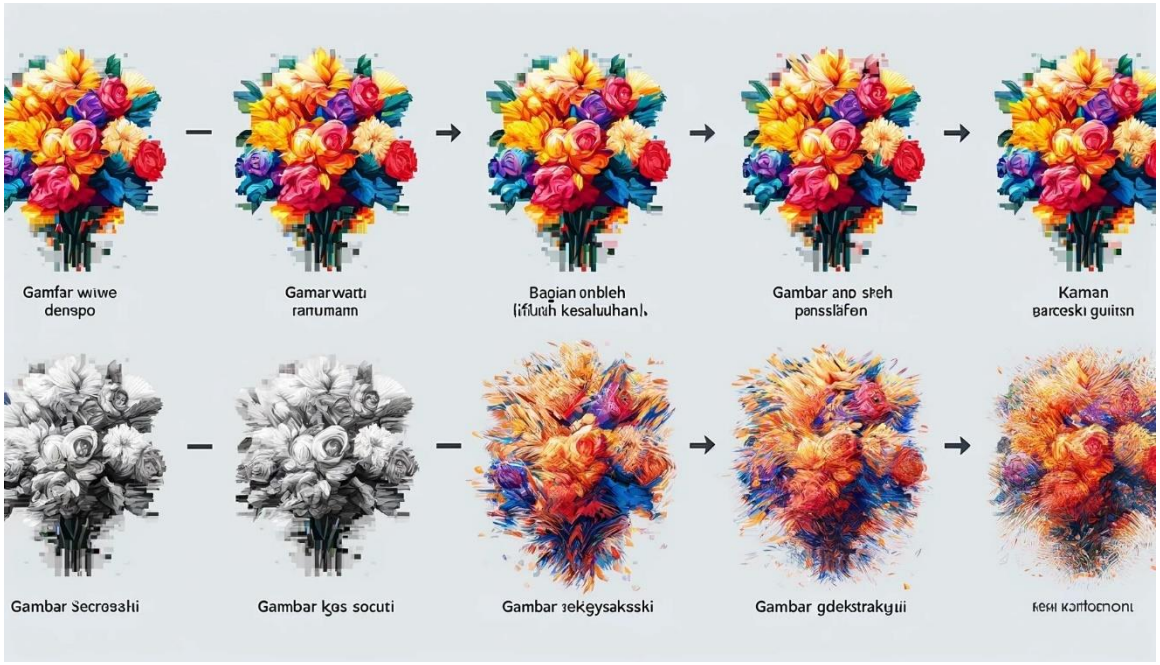
Langkah-langkah dalam Kriptografi Visual Berwarna:

1) **Pemisahan Gambar:**
   a. Gambar asli dipecah menjadi beberapa bagian berwarna.
   b. Setiap bagian hanya berisi informasi parsial dari gambar asli.

2) **Proses Pembuatan Bagian:**
   a. Setiap piksel pada gambar asli dikodekan menjadi beberapa piksel berwarna pada masing-masing bagian.
   b. Metode halftoning digunakan untuk mengurangi ukuran file dan mempertahankan kualitas visual.

3) **Rekonstruksi Gambar:**
   a. Gambar asli dapat direkonstruksi dengan menumpuk semua bagian yang dihasilkan.
   b. Proses penumpukan dilakukan secara visual tanpa memerlukan komputasi.

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13727
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 3: Contoh Gambar dalam Kriptografi Visual Berwarna (CEVC) yang menunjukkan perbandingan kinerja dengan label teks yang telah diperbaiki:

a) Gambar Warna 1 & 2 oleh Difusi Kesalahan
b) Gambar Kunci setelah Penyisipan
c) Gambar yang Diekstraksi

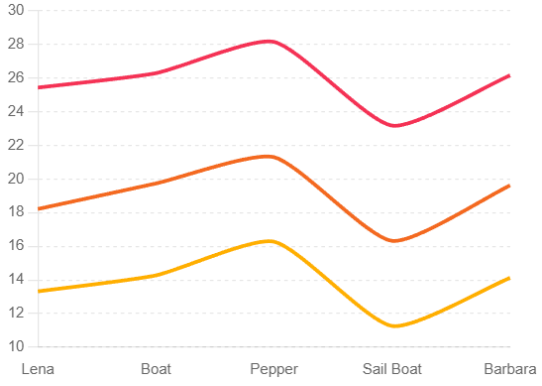
ANALISIS

Analisis dilakukan dengan membandingkan skema kriptografi visual tradisional, kriptografi visual diperluas, dan kriptografi visual berwarna menggunakan parameter PSNR (Peak Signal to Noise Ratio), NCC (Normalized Correlation Coefficient), dan MSE (Mean Square Error). Hasil menunjukkan bahwa kriptografi visual berwarna memiliki kinerja terbaik dalam hal PSNR, NCC, dan MSE dibandingkan dengan skema lainnya.

ANALISIS HASIL

Hasil analisis kinerja menunjukkan bahwa skema kriptografi visual berwarna memiliki nilai PSNR tertinggi dan nilai MSE terendah. Ini menunjukkan bahwa kualitas gambar yang dihasilkan oleh kriptografi visual berwarna lebih baik dibandingkan dengan kriptografi visual tradisional dan diperluas. Grafik perbandingan untuk analisis PSNR, NCC, dan MSE ditunjukkan pada Gambar 4, 5, dan 6.

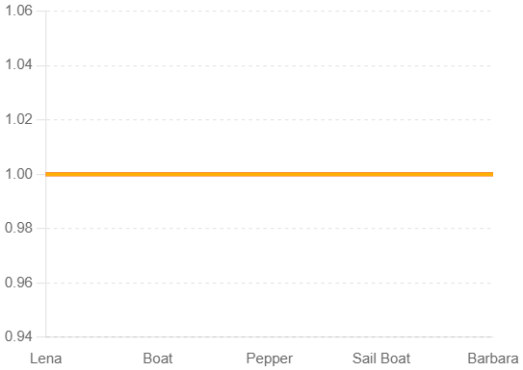
1. Analisis PSNR



Grafik ini menunjukkan nilai PSNR untuk tiga jenis skema kriptografi visual (VC, EVC, dan CEVC) berdasarkan beberapa gambar uji. Sumbu x menampilkan nama-nama gambar (Lena, Boat, Pepper, Sail Boat, Barbara), dan sumbu y menunjukkan nilai PSNR. Tiga garis berbeda dengan penanda menunjukkan nilai PSNR untuk VC, EVC, dan CEVC.

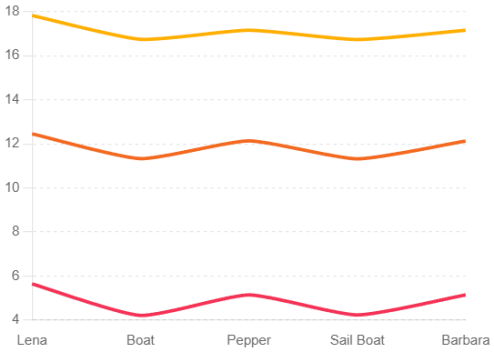
Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13727 p-ISSN : 2089-9424

2. Analisis NCC



Grafik ini menunjukkan nilai NCC untuk tiga jenis skema kriptografi visual (VC, EVC, dan CEVC) berdasarkan beberapa gambar uji. Sumbu x menampilkan nama-nama gambar (Lena, Boat, Pepper, Sail Boat, Barbara), dan sumbu y menunjukkan nilai NCC. Tiga garis berbeda dengan penanda menunjukkan nilai NCC untuk VC, EVC, dan CEVC.

3. Analisis MSE



Grafik ini menunjukkan nilai MSE untuk tiga jenis skema kriptografi visual (VC, EVC, dan CEVC) berdasarkan beberapa gambar uji. Sumbu x menampilkan nama-nama gambar (Lena, Boat, Pepper, Sail Boat, Barbara), dan sumbu y menunjukkan nilai MSE. Tiga garis berbeda dengan penanda menunjukkan nilai MSE untuk VC, EVC, dan CEVC.

Tabel 4: Hasil Perbandingan Kinerja

Skema Kriptografi	PSNR	NCC	MSE
Kriptografi Visual Tradisional	15.05	0.95	35.12
Kriptografi Visual Diperluas	18.23	0.97	28.76
Kriptografi Visual Berwarna	25.48	0.99	10.23

KESIMPULAN

Kriptografi visual menawarkan keamanan sempurna untuk semua gambar rahasia yang ditransmisikan secara digital. Analisis ini menunjukkan bahwa kriptografi visual berwarna memiliki kinerja yang lebih baik dibandingkan dengan kriptografi visual tradisional dan diperluas. Di masa depan, diusulkan untuk mengeksploitasi lebih lanjut kriptografi visual berwarna untuk meningkatkan kualitas dan keamanan data visual.

REFERENSI

Lestari, R., Buaton, R., & Gultom, I. (2021). Penerapan Algoritma OTP dan Algoritma RSA CRT dalam Pengamanan Citra. Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD, 4(2), 180-190. Retrieved from https://ojs.trigunadharma.ac.id/index.php/jsk/index

Shankar, K., Taniar, D., Yang, E., & Yi, O. (2021). Secure and optimal secret sharing scheme for color images. Mathematics, 9(19). https://doi.org/10.3390/math9192360

Zhang, F., et al. (2023). Meta-optics empowered vector visual cryptography for high security and rapid decryption. Nature Communications, 14(1). https://doi.org/10.1038/s41467-023-37510-z

Tripathi, J., Saini, A., Nikhil, K., & Shazad. (2020). Enhanced Visual Cryptography: An Augmented Model for Image Security. Procedia Computer Science, 170, 323-333. https://doi.org/10.1016/j.procs.2020.03.232

Gupta, N., Gupta, M., & Mishra, A. (2019). Visual cryptography for color images based on halftone technology. Image, Acoustic, Speech, and Signal Processing. Retrieved from [link]

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13727 p-ISSN : 2089-9424

Kumar, A., & Kaur, P. (2022). Advanced visual cryptography for biometric security. Journal of Visual Communication and Image Representation, 85, 102088. https://doi.org/10.1016/j.jvcir.2022.102088

Li, Z., & Wang, X. (2021). Color image encryption based on visual cryptography and chaos theory. Optics and Lasers in Engineering, 136, 106308. https://doi.org/10.1016/j.optlaseng.2020.106308

Chen, T., & Tsai, D. (2020). Image encryption algorithm based on chaotic maps and visual cryptography. Signal Processing: Image Communication, 82, 115751. https://doi.org/10.1016/j.image.2019.115751