



**ANALISIS *STRONG RAINBOW* ANTIMAGIC COLORING DAN
IMPLEMENTASINYA DALAM ENKRIPSI CITRA RGB
MENGUNAKAN *STREAM CIPHER***

TESIS

Oleh

**Nur Mauliska
241820101003**

**KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS JEMBER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
JURUSAN MATEMATIKA
JEMBER
2026**



**ANALISIS *STRONG RAINBOW* ANTIMAGIC COLORING DAN
IMPLEMENTASINYA DALAM ENKRIPSI CITRA RGB
MENGUNAKAN *STREAM CIPHER***

*diajukan untuk memenuhi sebagian persyaratan memperoleh gelar Magister pada
Program Studi Magister Matematika*

TESIS

Oleh

**Nur Mauliska
241820101003**

**KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS JEMBER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
JURUSAN MATEMATIKA
JEMBER
2026**

PERSEMBAHAN

Dengan menyebut nama Allah yang Maha Pengasih dan Maha Penyayang serta sholawat dan salam selalu tercurahkan kepada Nabi Muhammad SAW, penulis persembahkan ungkapan kebahagiaan atas terselesaikannya tesis dan rasa terima kasih kepada:

1. Ibu saya, Iin Nurhayati, Bapak saya, Miskat, adik saya, serta seluruh keluarga yang telah memberikan doa, dukungan, dan motivasi kepada penulis selama menempuh studi hingga penyelesaian tesis ini;
2. Ibu Dr. Ika Hesti Agustin, S.Si., M.Si selaku Dosen Pembimbing Utama dan Bapak Prof. Dr. Kiswara Agung Santoso, S.Si., M.Kom. selaku Dosen Pembimbing Anggota yang senantiasa meluangkan waktu dalam memberikan pengarahan dan bimbingan hingga terselesaikannya penulisan tesis ini;
3. Bapak Drs. Moh. Hasan, M.Sc., Ph.D. selaku Dosen Penguji I dan Bapak Prof. Drs. I Made Tirta, M.Sc., Ph.D. selaku Dosen Penguji II yang telah memberikan kritik dan saran yang membangun dalam penyempurnaan tesis ini.

Semoga Allah SWT senantiasa melimpahkan rahmat, keberkahan, dan balasan terbaik atas segala doa, dukungan, bimbingan, serta kebaikan yang telah diberikan. *Aamiin ya Rabbal 'alamin.*

MOTTO

“Man Jadda Wa Jada, Man Shabara Zhafira.”

Siapa yang bersungguh-sungguh akan berhasil, siapa yang bersabar akan beruntung.

إِنَّ مَعَ الْعُسْرِ يُسْرًا ۖ

“Sesungguhnya bersama kesulitan ada kemudahan.”

— QS. Al-Insyirah: 6



PERNYATAAN ORISINALITAS

Saya yang bertanda tangan di bawah ini:

Nama: Nur Mauliska

NIM : 241820101003

Menyatakan dengan sesungguhnya bahwa tesis yang berjudul “Analisis *Strong Rainbow Antimagic Coloring* dan Implementasinya dalam Enkripsi Citra RGB Menggunakan *Stream Cipher*” adalah benar-benar hasil karya sendiri, kecuali jika dalam pengutipan substansi disebutkan sumbernya, dan belum pernah diajukan pada institusi manapun, serta bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, 22 Juli 2026

Yang menyatakan,



Nur Mauliska

NIM. 241820101003

HALAMAN PERSETUJUAN

Tesis berjudul *Analisis Strong Rainbow Antimagic Coloring* dan Implementasinya dalam Enkripsi Citra RGB Menggunakan *Stream Cipher* telah diuji dan disetujui pada

Hari :

Tanggal :

Tempat : Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Jember

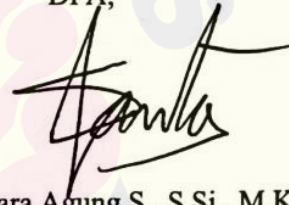
Tim Penguji

DPU,



Dr. Ika Hesti Agustin, S.Si., M.Si
NIP.198408012008012006

DPA,



Prof. Dr. Kiswara Agung S., S.Si., M.Kom.
NIP.197209071998031003

Penguji I,



Drs. Moh. Hasan, M.Sc., Ph.D.
NIP.196404041988021001

Penguji II,



Prof. Drs. I Made Tirta, M.Sc., Ph.D.
NIP.195912201985031002

ABSTRACT

The rapid development of digital technology has increased the need for methods to secure visual data, particularly digital images that may contain sensitive information. One approach to image security is encryption using a stream cipher, whose security level largely depends on the keystream employed. This study aims to determine the strong rainbow antimagic connection number of the wheel graph (W_n), helm graph (H_n), shell-butterfly graph ($BF_{2,n}$), octopus graph (O_n), and lotus graph (L_n), and to apply the weights obtained from Strong Rainbow Antimagic Coloring (SRAC) as a keystream for the encryption and decryption of RGB images using a stream cipher. The research adopts a theoretical-computational approach. The theoretical approach includes graph structure analysis, construction of bijective vertex labeling, determination of edge weights, verification of geodesic, and derivation of the lower and upper bounds of $srac(G)$. The computational approach constructs a keystream from the SRAC edge weights using the cyclic repetition method, which is then applied to the encryption process through a 4–4 bit swap operation followed by the XOR operation, while the decryption process is performed using XOR followed by the inverse swap operation. The results show that $srac(W_n) = n + 1$ for $n \geq 3$, $srac(H_n) \leq 2n - \left\lfloor \frac{n+1}{5} \right\rfloor$ for $n \geq 4$, $srac(BF_{2,n}) = 2n + 2$ for $n \geq 4$, $srac(O_n) = 2n$ for $n \geq 2$, and $srac(L_n) = n + 1$ for $n \geq 2$. The implementation of SRAC weights as a keystream demonstrates that the encrypted image undergoes significant visual randomization, while the decrypted image can be successfully recovered with a very high degree of similarity to the original image. Performance evaluation yields PSNR values ranging from 94.8919 dB to 95.3345 dB and UACI values close to 50%. These findings indicate that SRAC edge weights have strong potential as a mathematical construction for keystream generation in stream cipher-based digital image encryption.

Keywords: RGB image, keystream, Strong Rainbow Antimagic Coloring, stream cipher, graph theory.

RINGKASAN

Analisis *Strong Rainbow Antimagic Coloring* dan Implementasinya dalam Enkripsi Citra RGB Menggunakan *Stream Cipher*; Nur Mauliska, 241820101003; 2026; 56 Halaman; Program Studi Magister Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Penelitian ini membahas tentang *strong rainbow antimagic coloring* (SRAC), yaitu pengembangan dari *rainbow antimagic coloring* dengan syarat bahwa lintasan pelangi yang menghubungkan setiap pasangan titik harus merupakan lintasan terpendek (*geodesic*). Penelitian ini bertujuan menentukan nilai *strong rainbow antimagic connection number* $srac(G)$ pada beberapa kelas graf sekaligus mengimplementasikan bobot SRAC sebagai *keystream* dalam sistem enkripsi dan dekripsi citra berbasis *stream cipher*.

Objek penelitian meliputi lima kelas graf, yaitu graf roda W_n , graf helm H_n , graf *shell-butterfly* $BF_{2,n}$, graf *octopus* O_n , dan graf lotus L_n . Nilai $srac(G)$ diperoleh melalui konstruksi pelabelan titik secara bijektif, penentuan bobot sisi, analisis lintasan pelangi terpendek, serta pembuktian batas bawah dan batas atas.

Hasil penelitian menghasilkan teorema sebagai berikut.

1. *Strong rainbow connection number* dari $BF_{2,n}$ dengan $n \geq 4$ adalah $src(BF_{2,n}) = 2n + 2$;
2. *Strong rainbow connection number* dari O_n dengan $n \geq 2$ adalah $src(O_n) = 2n$;
3. *Strong rainbow connection number* dari L_n dengan $n \geq 2$ adalah $src(L_n) = n + 1$;
4. *Strong rainbow antimagic connection number* dari W_n untuk $n \geq 3$ adalah $srac(W_n) = n + 1$;
5. *Strong rainbow antimagic connection number* dari H_n dengan $n \geq 4$ adalah $srac(H_n) \leq 2n - \left\lfloor \frac{n+1}{5} \right\rfloor$;

6. *Strong rainbow antimagic connection number* dari $BF_{2,n}$ dengan $n \geq 4$ adalah $srac(BF_{2,n}) = 2n + 2$;
7. *Strong rainbow antimagic connection number* dari O_n dengan $n \geq 2$ adalah $srac(O_n) = 2n$
8. *Strong rainbow antimagic connection number* dari L_n dengan $n \geq 2$ adalah $srac(L_n) = n + 1$.

Bobot SRAC yang diperoleh selanjutnya digunakan sebagai *keystream* pada sistem *stream cipher*. Apabila jumlah bobot lebih sedikit daripada jumlah piksel citra, maka bobot diperluas menggunakan metode *cyclic repetition* hingga sesuai dengan ukuran data citra. Proses enkripsi dilakukan dalam dua tahap, yaitu *swap* 4–4 bit dan operasi *exclusive OR* (XOR) antara data hasil *swap* dengan *keystream* berbasis SRAC. Proses dekripsi dilakukan dengan tahapan yang berlawanan menggunakan *keystream* yang sama.

Implementasi dilakukan menggunakan Python 3 pada Google Colab dengan objek uji berupa citra Liska berformat JPEG. Pengujian menggunakan *keystream* dari kelima kelas graf menunjukkan bahwa seluruh metode mampu menghasilkan *cipher image* yang berbeda secara visual dari *plain image*, sehingga informasi citra berhasil disamarkan. Evaluasi menggunakan histogram, *Mean Squared Error* (MSE), *Peak Signal-to-Noise Ratio* (PSNR), dan *Unified Average Changing Intensity* (UACI) menunjukkan bahwa seluruh *keystream* berbasis SRAC mampu menghasilkan proses enkripsi dan dekripsi yang baik. Nilai UACI mendekati 50% menunjukkan perubahan intensitas piksel yang tinggi, sedangkan hasil dekripsi memiliki nilai MSE yang sangat kecil dan PSNR berkisar 94,8919 – 95,3345 dB, sehingga citra hasil dekripsi memiliki tingkat kemiripan yang sangat tinggi dengan citra asli.

Hasil penelitian menunjukkan bahwa bobot *strong rainbow antimagic coloring* pada graf roda, graf helm, graf *shell-butterfly*, graf *octopus*, dan graf lotus dapat dimanfaatkan sebagai *keystream* pada skema *stream cipher*. Selain menghasilkan nilai teoritis baru pada teori graf, penelitian ini juga menunjukkan bahwa bobot SRAC efektif diterapkan dalam sistem enkripsi dan dekripsi citra digital.

PRAKATA

Puji syukur ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tesis berjudul “Analisis *Strong Rainbow Antimagic Coloring* dan Implementasinya dalam Enkripsi Citra RGB Menggunakan *Stream Cipher*”. Penelitian ini diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan Pendidikan strats dua (S2) pada Program Studi Magister Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Penyusunan tesis ini tidak lepas dari bantuan berbagai pihak. Oleh karena itu, penulis menyampaikan terimakasih kepada:

1. Ibu Dr. Ika Hesti Agustin, S.Si., M.Si selaku Dosen Pembimbing Utama dan Bapak Prof. Dr. Kiswara Agung Santoso, S.Si., M.Kom. selaku Dosen Pembimbing Anggota yang senantiasa meluangkan waktu dalam memberikan pengarahan dan bimbingan hingga terselesaikannya penulisan tesis ini;
2. Bapak Drs. Moh. Hasan, M.Sc., Ph.D. selaku Dosen Penguji I dan Bapak Prof. Drs. I Made Tirta, M.Sc., Ph.D. selaku Dosen Penguji II yang telah memberikan kritik dan saran yang membangun dalam penyempurnaan tesis ini;
3. Seluruh teman-teman CGANT yang telah membagikan ilmu dan pengalaman berharga serta mengajarkan bahwa sebuah perbedaan bukanlah alasan untuk tidak saling membantu;
4. Almamater tercinta Program Studi Magister Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember;
5. Semua pihak yang telah membantu terselesaikannya tesis ini.

Penulis juga menerima segala kritik dan saran dari semua pihak demi kesempurnaan tesis ini. Akhirnya penulis berharap, semoga tesis ini dapat bermanfaat.

Jember, 18 Juli 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
PERSEMBAHAN.....	iii
MOTTO	iv
PERNYATAAN ORISINALITAS.....	v
HALAMAN PERSETUJUAN	vi
ABSTRAK	vii
RINGKASAN	viii
PRAKATA	x
DAFTAR ISI.....	v
DAFTAR TABEL	vii
DAFTAR GAMBAR.....	viii
DAFTAR LAMPIRAN	ix
DAFTAR NOTASI.....	x
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian	3
1.4 Manfaat Penelitian	3
1.5 Kebaharuan	4
BAB 2. TINJAUAN PUSTAKA.....	5
2.1. Terminologi Graf	5
2.2. Deskripsi dan Struktur Graf	6
2.3. <i>Rainbow Coloring</i> dan <i>Strong Rainbow Coloring</i>	7
2.4. <i>Rainbow Antimagic Coloring</i> (RAC) dan <i>Strong Rainbow Antimagic Coloring</i> (SRAC)	8
2.5. Citra RGB.....	9
2.6. <i>Stream Cipher</i> pada Enkripsi dan Dekripsi Citra RGB	10
2.7. Evaluasi Kinerja Metode	12
2.8. Hasil Penelitian Terdahulu	13
BAB 3. METODOLOGI PENELITIAN.....	15
3.1 Subjek Penelitian.....	15
3.2 Metode Analisis	15
3.3 Prosedur Penelitian.....	17
BAB 4. HASIL DAN PEMBAHASAN.....	19

4.1	Nilai <i>Strong Rainbow Coloring</i> (SRC)	19
4.1.1	<i>Strong Rainbow Coloring</i> pada Graf <i>Shell-Butterfly</i>	19
4.1.2	<i>Strong Rainbow Coloring</i> pada Graf <i>Octopus</i>	20
4.1.3	<i>Strong Rainbow Coloring</i> pada Graf <i>Lotus</i>	21
4.2	Nilai <i>Strong Rainbow Antimagic Coloring</i> (SRAC).....	22
4.2.1	<i>Strong Rainbow Antimagic Coloring</i> pada Graf <i>Roda</i>	22
4.2.2	<i>Strong Rainbow Antimagic Coloring</i> pada Graf <i>Helm</i>	28
4.2.3	<i>Strong Rainbow Antimagic Coloring</i> pada Graf <i>Shell-Butterfly</i> .	35
4.2.4	<i>Strong Rainbow Antimagic Coloring</i> pada Graf <i>Octopus</i>	42
4.2.5	<i>Strong Rainbow Antimagic Coloring</i> pada Graf <i>Lotus</i>	45
4.3	Implementasi Bobot SRAC sebagai <i>Keystream</i> pada <i>Stream Cipher</i>	47
4.3.1	Konstruksi Bobot SRAC sebagai <i>Keystream</i>	48
4.3.2	Proses Enkripsi	49
4.3.3	Proses Dekripsi.....	51
4.3.4	Analisis Hasil Enkripsi dan Dekripsi	52
BAB 5. KESIMPULAN DAN SARAN		54
5.1	Kesimpulan	54
5.2	Saran.....	54
DAFTAR PUSTAKA		55

DAFTAR TABEL

Tabel 2.1 Nilai kebenaran operasi XOR	11
Tabel 2.2 Penelitian terdahulu $src(G)$	13
Tabel 2.3 Penelitian terdahulu $srac(G)$	14
Tabel 4.1 Lintasan <i>strong rainbow</i> setiap dua simpul pada graf roda	27
Tabel 4.2 Lintasan <i>strong rainbow</i> setiap dua simpul pada graf helm	34
Tabel 4.3 Lintasan <i>strong rainbow</i> setiap dua simpul pada graf <i>shell-butterfly</i> ...	41
Tabel 4.4 Lintasan <i>strong rainbow</i> setiap dua simpul pada graf <i>octopus</i>	44
Tabel 4.5 Lintasan <i>strong rainbow</i> setiap dua simpul pada graf lotus	47
Tabel 4.6 Matriks <i>pixel RGB plain image</i> berukuran 5×5	48
Tabel 4.7 Perhitungan proses enkripsi pada baris kelima	50
Tabel 4.8 Perhitungan proses dekripsi pada baris kelima	51
Tabel 4.9 Analisis <i>cipher image</i>	53

DAFTAR GAMBAR

Gambar 2.1 Contoh graf G	5
Gambar 2.2 Enkripsi dan Dekripsi	12
Gambar 3.1 Bagan penelitian	18
Gambar 4.1 <i>Strong rainbow antimagic coloring</i> pada graf roda W_{16}	27
Gambar 4.2 <i>Strong rainbow antimagic coloring</i> pada graf helm H_{12}	34
Gambar 4.3 <i>Strong rainbow antimagic coloring</i> pada graf <i>shell-butterfly</i> $BF_{2,8}$.	41
Gambar 4.4 <i>Strong rainbow antimagic coloring</i> pada graf <i>octopus</i> O_7	44
Gambar 4.5 <i>Strong rainbow antimagic coloring</i> pada graf lotus L_7	47
Gambar 4.6 <i>Plain image</i> Liska	48
Gambar 4.7 <i>Cipher image</i>	50
Gambar 4.8 Hasil implementasi enkripsi dan dekripsi <i>plain image</i> Liska	52

DAFTAR LAMPIRAN

- Lampiran 1. Gambar graf roda W_n , graf helm H_n , graf *shell-butterfly* BF_n , graf *octopus* O_n , atau graf lotus L_n
- Lampiran 2. *Strong rainbow coloring* pada graf *shell-butterfly* $BF_{2,4}$, graf *octopus* O_4 , dan graf lotus L_4
- Lampiran 3. Perhitungan manual proses enkripsi dengan operasi XOR
- Lampiran 4. Perhitungan manual proses dekripsi dengan operasi XOR
- Lampiran 5. Hasil pengenkripsian dan pendekripsian
- Lampiran 6. Skrip program pada *software* Python 3 (Google Colab)



DAFTAR NOTASI

G	= Graf G
$V(G)$	= Himpunan titik (<i>vertex</i>) pada graf G
$E(G)$	= Himpunan sisi (<i>edge</i>) pada graf G
$ V(G) $	= Banyaknya titik pada graf G
$ E(G) $	= Banyaknya sisi pada graf G
(u, v)	= Titik-titik pada graf G
(uv)	= Sisi yang menghubungkan titik u dan v
$d(v)$	= Derajat titik v
$\Delta(G)$	= Derajat maksimum graf G
$d(u, v)$	= Jarak titik u dan v , lintasan uv terpendek
$diam(G)$	= Diameter graf G
P	= Lintasan (<i>path</i>) pada graf
C_n	= Graf siklus dengan n titik
W_n	= Graf roda (<i>wheel graph</i>) dengan n titik pada siklus luar
H_n	= Graf helm (<i>helm graph</i>)
$BF_{2,n}$	= Graf <i>shell-butterfly</i>
O_n	= Graf <i>octopus</i>
L_n	= Graf <i>lotus</i>
c	= Fungsi pewarnaan sisi graf
k	= Banyaknya warna yang digunakan dalam suatu pewarnaan
$rc(G)$	= <i>Rainbow connection number</i> dari graf G
$src(G)$	= <i>Strong rainbow connection number</i> dari graf G
$rac(G)$	= <i>Rainbow antimagic connection number</i> dari graf G
$srac(G)$	= <i>Strong rainbow antimagic connection number</i> dari graf G
M	= Banyaknya baris atau tinggi citra digital
N	= Banyaknya kolom atau lebar citra digital
i	= Indeks baris piksel atau indeks elemen
j	= Indeks kolom piksel
$c \in \{R, G, B\}$	= Indeks kanal warna pada citra RGB
P_R	= Matriks piksel kanal merah pada citra asli
P_G	= Matriks piksel kanal hijau pada citra asli
P_B	= Matriks piksel kanal biru pada citra asli
P_i	= Elemen atau byte <i>plaintext</i> ke- i
K_i	= Elemen <i>keystream</i> ke- i

C_i	= Elemen atau byte <i>ciphertext</i> ke- i
D_i	= Elemen hasil dekripsi ke- i
$P_c(i, j)$	= Nilai piksel <i>plaintext</i> pada posisi (i, j) dan kanal c
$K_c(i, j)$	= Nilai <i>keystream</i> pada posisi (i, j) dan kanal c
$C_c(i, j)$	= Nilai piksel <i>ciphertext</i> pada posisi (i, j) dan kanal c
$D_c(i, j)$	= Nilai piksel hasil dekripsi pada posisi (i, j) dan kanal c
$\oplus$	= Operasi <i>exclusive OR</i> (XOR)
$\emptyset$	= Himpunan kosong
MSE	= <i>Mean Squared Error</i>
PSNR	= <i>Peak Signal-to-Noise Ratio</i>
UACI	= <i>Unified Average Changing Intensity</i>
RGB	= <i>Red, Green, Blue</i>
SRAC	= <i>Strong Rainbow Antimagic Coloring</i>
RAC	= <i>Rainbow Antimagic Coloring</i>
XOR	= <i>Exclusive OR</i>