Journal of Computer Science

Original Research Paper

Irregular Reflexive Labeling and Elementary Row Operations for Enhanced Biometric Image Encryption

[1,2]Ika Hesti Agustin, [1,2]Dafik, [1]Rifki Ilham Baihaki, [1,3]Marsidi and [1,2]Kiswara Agung Santoso

[1]PUI-PT Combinatorics and Graph, CGANT-University of Jember, Indonesia
[2]Department of Mathematics, Faculty of Mathematics and Natural Sciences, University of Jember, Indonesia
[3]Department of Mathematics Education, Faculty of Teacher Training and Education, Universitas PGRI Argopuro Jember, Indonesia

Article history
Received: 03-04-2024
Revised: 06-06-2024
Accepted: 24-06-2024

Corresponding Authors:
Ika Hesti Agustin
Department of Mathematics, Faculty of Mathematics and Natural Sciences, University of Jember, Indonesia
Email: ikahesti.fmipa@unej.ac.id

Abstract: A total k-labeling defined the function f_e: $E(G) \rightarrow \{1, 2, \ldots, k_e\}$ and f_v: $V(G) \rightarrow \{0, 2, \ldots, 2k_v\}$, where, $k = \max\{k_e, 2k_v\}$. For graph G, the total k-labeling is called an edge (or a vertex) irregular reflexive k-labeling if the condition of every two different edges (or vertices) has different weights. The smallest value of k for which such labeling exists is called the reflexive edge strength (or reflexive vertex strength) of the graph G, denoted by *res* (G) (or *rvs*(G)). This research objective is developing edge irregular reflexive k-labeling and combining edge and vertex irregular reflexive k-labeling and row element operation as an innovative approach to constructing a robust keystream for biometric image encryption. The results show that the best keystream is generated by $C_n \odot P_2$ and the complete graph. Our results can also surpass existing encryption algorithms such as AES and DES.

Keywords: Biometrics Image, Image Encryption, Irregular Reflexive k-Labeling, Elementary Row Operation

Introduction

Irregularity labeling is the labeling of a graph element using consecutive positive integers, which may be repeated. The theory of irregularity labeling was introduced by Chartrand *et al*. (1988) and is known as irregularity strength ($s(G)$). This concept was further explored by subsequent researchers. Based on this research, (Bača *et al*., 2007) developed two parameters, namely the total edge irregularity strength (*tes(G)*) and the total vertex irregularity strength (*tvs*(G)) in graphs. Furthermore, (Marzuki *et al*., 2013) introduced the total irregularity strength (*ts*(G)), which combines the concepts of *total edge irregularity strength* (*tes*(G)) and total vertex irregularity strength (*tvs*(G)). Ahmad *et al*. (2014) defined the edge irregularity strength (*es*(G)). (Bača *et al*., 2007) initiated research on the total labeling of k-irregular edges. Ahmad *et al*. (2014) researched on k-irregular edge labeling on various graphs including paths, cycles, stars, double stars, and graphs resulting from the cartesian product $P_m \times P_n$. In 2018, they extended their research to include and complete ternary trees. Additional research on k-irregular edge labeling can be found in (Ibrahim *et al*., 2020; Tarawneh *et al*.., 2018; 2020; Susanti *et al*., 2020; Putra and Susanti, 2018; Ratnasari and Susanti, 2020).

Furthermore, the concept of irregular labeling was developed on k-labeling by Tanna *et al*. (2020). A graph G is a non-empty object consisting of a set of vertices V and edges E (Guirao *et al*., 2018). If a graph G has a set of vertices $V(G)$ and a set of edges $E(G)$, then we write $G = (V(G), E(G))$ (Ahmad *et al*., 2022; Maryati *et al*., 2020). A total k-labeling is defined as an irregular edge total k-labeling of graph G if every two distinct edges have different weights (Agustin *et al*., 2021). The edge weight is the sum of the labels of its incident vertices and the label of that edge. Bača extended the above notion into an edge irregular reflexive k-labeling (Agustin *et al*., 2020).

The total k-labeling is defined by the function f_e: $E(G) \rightarrow 1, 2, ..., ke$ and f_v: $V G$: The total $V(G) \rightarrow k$-labeling is, $2, 2k_v$, where, k = max called an edge irregular reflexive k-labeling if every two different edges x_1x_2 and y_1y_2 of G satisfy $wt\ (x_1x_2) \neq wt\ (y_1y_2)$, where, $wt\ (x_1x_2) = f_v\ (x_1) + f_e\ (x_1x_2) + f_v(x_2)$ (Agustin *et al*., 2021). The smallest value of k for which such labeling exists is called the reflexive edge strength of the graph G, denoted by *res* (G) (Alfarisi *et al*., 2021; Bača *et al*., 2017). Some lemmas on˘ the lower bound for *res* (G) can be seen in (Agustin *et al*., 2021; Bača *et al*., 2017; 2019).

Meanwhile, a total labeling *h* total: V (*k*-labeling of the graph) $\cup E$ $(G) \rightarrow$ 1, 2, 3, ..., *k* is called a vertex irregular total *k*-labeling of the graph *G* if for every two vertices *u*, $v \in V(G)$, where, $u \neq v$, $wit_h(u) \neq wit_h(v)$, where the vertex weight $wit_h(u) = h(u) + \Sigma_{uv \in E(G)} h(uv)$ (Agustin *et al*., 2023). The total vertex irregularity strength, denoted by $tvs(G)$, is the minimum *k* for which graph *G* has a vertex irregular total *k*-labeling (Alfarisi *et al*., 2021). Some research results on vertex irregular reflexive *k*-labelling and edge irregular reflexive *k*-labelling can be seen in Table (1).

Some important applications of graph labeling include social network analysis, product recommendation, network optimization, task scheduling, supply management systems, image analysis, text and image encryption, etc. Prihandoko *et al*., 2022; Maryati *et al*., 2020; Su *et al*., 2020). The development of irregular reflexive *k*-labeling theory has been a significant breakthrough in the field of cryptography, particularly in biometric data encryption applications. By utilizing the complex concepts of this theory, researchers can design stronger and more secure encryption systems to protect sensitive biometric data, such as fingerprints, retinal scans, and facial recognition.

Our focus is on biometric data protection. Encrypting biometric data using irregular reflexive *k*-labeling theory allows information to be transformed into a form that cannot be read or understood without a suitable decryption key (Wen *et al*., 2021). In this research, we use some previously published irregular reflexive *k*-labeling theorems to construct keystreams as an encryption method. Additionally, as a novelty in this research, we develop a new theorem of edge irregular reflexive *k*-labeling and combine edge and vertex irregular reflexive *k*-labeling with row element operation as an innovative approach to construct robust keystreams for image encryption. The purpose of using this labeling is to strengthen the encryption method so that the security of biometric data is more guaranteed.

Thus, the integration of this theory into biometric data encryption applications paves the way for more advanced and reliable security systems in a variety of contexts, including applications involving high-level security, such as user-on-identification smart devices or sensitive medical data.

In addition, we introduce the theory of row element operations as an innovative approach in the field of cryptography. Irregular reflexive *k*-labeling theory is used to design strong and unpredictable encryption schemes for biometric data, while row element operations are applied to improve the efficiency and speed of encryption and decryption processes. By combining these two techniques, biometric information can be converted into an encrypted format with a high level of security while maintaining efficient computational performance.

Table 1: The previous results on irregular reflexive *k* labeling

Vertex irregular reflexive graph	Edge irregular reflexive graph
Sunlet S_n (Agustin *et al*., 2020)	Prism (D_n) (Tanna *et al*., 2020)
Helm (H_n) (Agustin *et al*., 2020)	Wheel (W_n) (Tanna *et al*., 2020)
Subdivided Star (SS) (Agustin *et al*., 2020)	Fan (F_n) (Tanna *et al*., 2020)
Broom ($Br_{n,m}$) (Agustin *et al*., 2020)	Basket (B_n) (Tanna *et al*., 2020)
Prism (D_n) (Tanna *et al*., 2020)	Generalized Friendship (Bača *et al*., 2017)
Wheel (W_n) (Tanna *et al*., 2020)	Disjoint Union Generalized Petersen Gui siklus (C_n) (Bača *et al*., 2019)
Fan (F_n) (Tanna *et al*., 2020)	Cycle Cartesian Operation $C_n \times C_3$ (Bača *et al*., 2019)
Basket (B_n) (Tanna *et al*., 2020)	(P_n +(2*K*1), C_n +(2*K*1)) (Bača *et al*., 2019)
Cycle (C_n) (Agustin *et al*., 2020)	Peneralized Sub-Divided Star (Agustin *et al*., 2021)
Generalized Friendship ($F_{n,m}$) (Agustin *et al*., 2020)	Broom (Agustin *et al*., 2021)
Complete (K_n) (Agustin *et al*. (2020)	Double Star ($DS_{m,n}$) (Agustin *et al*., 2021)
Gear (G_n) (Alfarisi *et al*., 2021)	Corona of the Path (Indriati *et al*., 2020)
Book (B_n) (Alfarisi *et al*., 2021)	Disjoint Wheel-Relate (Zhang *et al*., 2018)
Triangular Book (Bt_n) (Alfarisi *et al*., 2021)	Disjoint Specifically Gear (Zhang *et al*., 2018)
Disjoint Union of Gear (Alfarisi *et al*., 2021)	Disjoint Prism (Zhang *et al*., 2018)
Ladder (L_n) (Agustin *et al*., 2021b)	Corona Product of Two Paths (Yoong *et al*., 2021)
Complete ($K_{2,n}$) (Agustin *et al*., 2021b)	Corona Product of a Path with Isolated Vertices (Yoong *et al*., 2021)
Antiprism (An) (Agustin *et al*., 2022)	Star (Ibrahim *et al*., 2020)
Friendship (Fr_n) (Agustin *et al*., 2022)	Caterpillar (Ibrahim *et al*., 2020)
Double wheel (Dw_n) (Agustin *et al*., 2022)	Cartesian product of two paths and two cycles (Yongsheng *et al*., 2021)
	Ladder (Ln) (Agustin *et al*., 2021)
	Triangular Ladder (TL_n) (Agustin *et al*., 2021)
	$P_n \times C_3$ (Agustin *et al*., 2021)
	$P_n \odot P_2$ (Agustin *et al*., 2021)
	$P_n \odot C_3$ (Agustin *et al*., 2021)

DOI: 10.3844/jcssp.2024.1766.1777

We tested several Irregular Reflexive Labelling theorems to assess which algorithm provides the strongest encryption security. The parameters used to analyze the accuracy of the image encryption process include Peak Signal Noise Ratio (PSNR), United Average Changing Intensity (UACI), Number of Pixel Change Rate (NPCR), and Correlation. Here are some research questions from this study:

1. What is the RES value of the graph $C_n \odot P_2$ graph is used as one of the bases for $C_n \odot P_2$? The keystream formation in the encryption process
2. How do we construct the algorithm to build the keystream Irregular Reflexive *k* Labeling and encryption process algorithm?
3. How is the image encryption process with keystream developed from some theorems of vertex irregular reflexive *k* labeling and edge irregular reflexive *k* labeling?
4. What is the accuracy level of the image encryption process by using irregular reflexive *k* labeling? The accuracy level can be seen from PSNR, UACI, NPCR, and correlation in the image encryption process

Materials

We use a computer with Intel i5-11400H hardware, Nvidia Geforce RTX 3060 6 GB GPU, and 16 GB RAM. While the software we use is Matlab R2023b. We chose several biometric images from Kaggle, such as iris image (Mohammad, 2024), face images (we use our image), and fingerprint image (Kairess, 2022), see Fig. (1). Some of the tests we did include calculating the correlation values of grayscales level. In addition, we also analyze the calculation of the Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Peak Signal Noise Ratio (PSNR). We also analyze the image before and after encryption from the histogram. We also analyze our proposed encryption method from a security standpoint.

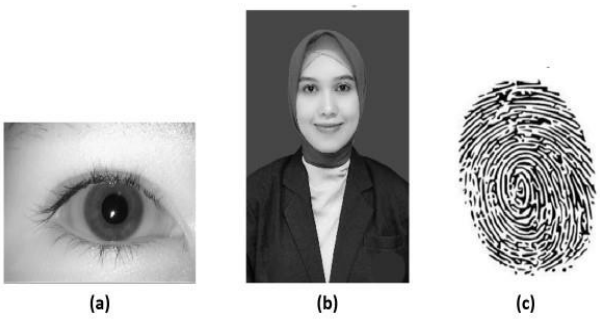

Fig. 1: A set of test images (a) Iris Eye, (b) face, (c) fingerprint

Methods

The encryption process using irregular reflexive *k* labeling and row elementary operations combines the advanced steps of both techniques to provide high security and efficiency in protecting data. Here are the steps in the encryption process:

1. Conversion of plain image (biometric data): The first step in the encryption process is to convert the plain image (biometric data) into an image matrix representation where the elements are in modulo 255. This conversion ensures that the image data is in a suitable format for subsequent operations. For example, if the original pixel value is 300, it will be converted to 45 (300 mod 255)
2. Labeling with Irregular Reflexive K-labeling: After converting the biometric data into a suitable format, we apply a labeling technique using irregular reflexive *k*-labeling theory. This step constructs a keystream analogous to an adjacency matrix, which will be used in the encryption process. The irregular reflexive *k*-labeling assigns labels to the graph vertices such that the labels of the vertices are distinct and the label of any vertex is reflexive
3. Elementary row operations: Elementary row operations are applied to the image matrix and the resulting adjacency matrix. The basic operations include row addition, which involves adding one row to another row; row swapping, which involves swapping two rows; row multiplication, which involves multiplying a row by a constant; and row combination, which involves adding a multiple of one row to another row. These operations enhance the security of the encryption by making the encrypted data more resistant to attacks
4. Encryption Process: Summation of image matrix and adjacency matrix that has been subjected to elementary row operations in modulo 255. This process aims to hide the information contained in the biometric data and make it difficult to understand without the right decryption key
5. Chipper Image: Once the encryption process is complete, the encrypted data is ready to be stored or shared with others. The data has been converted into a form that cannot be read or understood without using the appropriate decryption key

To evaluate the performance of our proposed cryptosystem method, we use several parameters, including the correlation test (*r*), NPCR, UACI, and PSNR.

Correlation Test (*r*): The correlation between the original image and the encrypted image is calculated using Eq. (1):

$$r=\frac{\sum_m\sum_n(A_{mn}-\bar{A})(B_{mn}-\bar{B})}{\sqrt{\sum_m\sum_n(A_{mn}-\bar{A})^2(\sum_m\sum_n(B_{mn}-\bar{B})^2)}} \quad (1)$$

where, A are red/green/blue component value of the plain image, B is the red/green/blue component value of the cipher image, $\bar{A}$ is the mean (A), $\bar{B}$ is the mean (B), m is the $m^{\text{-th}}$ pixel value, and n is $n^{\text{-th}}$ pixel value.

Number of Pixel Change Rate (NPCR): The Number of Pixel Change Rate (NPCR) is a metric used to evaluate the effectiveness of an image encryption algorithm by measuring the rate of change in pixel values between the original (plain) image and the encrypted (cipher) image. The NPCR is calculated using Eq. (2):

$$NPCR=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}Dij\times 100\% \quad (2)$$

where, H and W are the length and width of the color image respectively.

Unified Average Changing Intensity (UACI): A metric used to evaluate the performance of image encryption algorithms, specifically to measure their sensitivity to small changes in the plaintext image. The UACI is calculated using Eq. (3):

$$UACI=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(\frac{v(i,j)-v'(i,j)}{255})\times 100\% \quad (3)$$

where, H is the height of the image, W is the width of one of the images, v (i, j) is the pixel value of the cipher text image at position (i, j), v' (i, j) is the pixel value of the cipher text image generated from a slightly different plaintext image at the same position (i, j).

Peak Signal-to-Noise Ratio (PSNR): A widely used metric for assessing the quality of a reconstructed image compared to its original version. The PSNR is calculated using Eqs. (4-5):

$$PSNR=10\times\log_{10}\frac{255^2}{MSE}(dB) \quad (4)$$

$$MSE=\frac{1}{M\times N\times 3}\sum_{i=1}^{H}\sum_{j=1}^{W}\sum_{k=1}^{3}(P(i,j,k)-C(i,j,k)^2) \quad (5)$$

where, P is the plain image and C is the cipher image.

Results

The Irregular Reflexive K Labeling

We propose an image encryption process based on irregular reflexive k labeling. We use simple, nontrivial, non-empty, and connected graphs. For more detail on the notions, see (Ibrahim *et al*., 2020; Gallian, 2022). We construct keystreams based on the labeling theorems of reflexive irregular edge labeling k and reflexive irregular vertex labeling k on complete, subdivided star, helmet, $C_n\odot P_2$, broom, double star, and ladder graphs. We present a new theorem on reflexive irregular edge labeling on cycle product and path graphs. Let $C_n\odot P_2$ be a corona product of the cycle and path graph. For positive integers n ≥3:

$$res(C_n\odot P_2)=\begin{Bmatrix}\lceil\frac{4n}{3}\rceil+1, if 4n\equiv 2(mod\ 6)\\ \lceil\frac{4n}{3}\rceil, otherwise\end{Bmatrix}$$

Proof: Let Tl_n, $n\geq 3$, be a graph with the vertex set $V(C_n\odot P_2)=\{x_i: 1\leq i\leq 3n\}$, $|V(Tl_n)|=3n$ and the edge set $E(C_n\odot P_2)=\{x_{2i-1}x_{2i-1},\ x_{2i-1}x_{2n+i},\ x_{2i}x_{2n+i}: 1\leq i\leq n\}\cup\{x_{2n+i}x_{2n+i+1}: 1\leq i\leq n-1\}\cup\{x_{2n+1}x_{3n}\}$, $|E(C_n\odot P_2)|=4n$. Since $4n$ is an even integer, such that $4n\neq 3$ (mod 6). We have the lower bound lemma to determine the lower bound of $res(C_n\odot P_2)$ as follows:

$$res(C_n\odot P_2)\geq\begin{Bmatrix}\lceil\frac{4n}{3}\rceil+1, if 4n\equiv 2(mod\ 6)\\ \lceil\frac{4n}{3}\rceil, otherwise\end{Bmatrix}$$

Furthermore, we determine the upper bound of $res(C_n\odot P_2)$ by constructing the vertex labeling as follows.

For $1\leq i\leq 2n$, we have:

$$f_v(x_i)\begin{Bmatrix}0, & if\ i\in\{1,2\}\\ 2, & if\ i\in\{3,4\}\\ 4\lceil\frac{i-4}{6}\rceil, & if\ i\equiv 0,5(\mathrm{mod}\,6)\\ 4\lceil\frac{i-4}{6}\rceil+2, & if\ i\equiv 1,2,3,4(\mathrm{mod}\,6)\end{Bmatrix}$$

For $1\leq j\leq n$, we have:

$$f_v(x_{2n+j})\begin{Bmatrix}0, & if\ j\in\{1,2\}\\ 2, & if\ j\in\{3,4\}\\ 4\lceil\frac{i-2}{3}\rceil, & if\ j\equiv 0(\mathrm{mod}\,3)\\ 4\lceil\frac{i-2}{3}\rceil+2, & if\ j\equiv 1,2(\mathrm{mod}\,3)\end{Bmatrix}$$

Next, we construct the function of edge labeling as follows:

$$f_e(x_{2i-1}x_{2i})=\begin{Bmatrix}2, & if\ i=1\\ 4\left\lceil\frac{i-1}{3}\right\rceil-2, & if\ 2\le i\le\frac{2k}{4}\\ 4\left\lceil\frac{i-1}{3}\right\rceil-1, & if\ \frac{2k}{4}+1\le i\le n\end{Bmatrix}$$

$$f_e(x_{2i-1}x_{2n+1})=\begin{Bmatrix}1, & if\ i=1\\ 4\left\lceil\frac{i-1}{3}\right\rceil-3, & if\ 2\le i\le\frac{2k}{4}\\ 4\left\lceil\frac{i-1}{3}\right\rceil-2, & if\ \frac{2k}{4}+1\le i\le n\end{Bmatrix}$$

$$f_e(x_{2i}x_{2n+i})=\begin{Bmatrix}3, & if\ i=1\\ 4\left\lceil\frac{i-1}{3}\right\rceil-1, & if\ 2\le i\le\frac{2k}{4}\\ 4\left\lceil\frac{i-1}{3}\right\rceil, & if\ \frac{2k}{4}+1\le i\le n\end{Bmatrix}$$

$$f_e(x_{2n+i}x_{2n+i+1})=\begin{Bmatrix}2, & if\ i=1\\ 4\left\lceil\frac{i-1}{3}\right\rceil-2, & if\ i\equiv 0,2(\bmod 3),\ 2\le i\le\frac{2k}{4}-1\\ 4\left\lceil\frac{i-1}{3}\right\rceil, & if\ i\equiv 1(\bmod 3),\ 2\le i\le\frac{2k}{4}-1\\ 4\left\lceil\frac{i-1}{3}\right\rceil-1, & if\ i\equiv 0,2(\bmod 3),\ \frac{2k}{4}\le i\le n-1\\ 4\left\lceil\frac{i-1}{3}\right\rceil+1, & if\ i\equiv 1(\bmod 3),\ \frac{2k}{4}\le i\le n-1\end{Bmatrix}$$

$$f_e(x_{2n+1}x_{3n})=k$$

where:

$$k=\begin{Bmatrix}\left\lceil\frac{4n}{3}\right\rceil+1, & if\ 4n\equiv 2(\bmod 6)\\ \left\lceil\frac{4n}{3}\right\rceil, & otherwise\end{Bmatrix}$$

Based on the vertex and edge labeling, we have the edge weight sets as follows:

$$wt(x_{2i-1}x_{2i})=\begin{Bmatrix}4i-2, & if\ 1\le i\le\frac{2k}{4}\\ 4i-1, & if\ \frac{2k}{4}+1\le i\le n\end{Bmatrix}$$

$$wt(x_{2i-1}x_{2n+i})=\begin{Bmatrix}4i-3, & if\ 1\le i\le\frac{2k}{4}\\ 4i-2, & if\ \frac{2k}{4}+1\le i\le n\end{Bmatrix}$$

$$wt(x_{2i}x_{2n+i})=\begin{Bmatrix}4i-1, & if\ 1\le i\le\frac{2k}{4}\\ 4i, & if\ \frac{2k}{4}+1\le i\le n\end{Bmatrix}$$

$$wt(x_{2n+i}x_{2n+i+1})=\begin{Bmatrix}4i, & if\ 1\le i\le\frac{2k}{4}-1\\ 4i+1, & if\ \frac{2k}{4}\le i\le n-1\end{Bmatrix}$$

$$wt(x_{2n+1}x_{3n})=2k$$

It is easy to see that the edge weights in the edge weights sets above are all distinct. Since we have *res* $(C_n\odot P_2) \ge k$ and *res* $(C_n\odot P_2) \le k$, such that we conclude that *res* $(C_n\odot P_2) = k$. It completes the proof.

Algorithm of Keystream and Encryption Process

In this section, we will describe the keystream algorithm and encryption process used in maintaining data security. The keystream algorithm is at the core of the key generation that will be used in the encryption process, while the encryption algorithm plays an important role in keeping sensitive information confidential. By understanding these two processes well, a deeper insight into how data security systems can operate effectively will be gained.

Algorithm 1: Keystream Algorithm using Irregular Reflexive Labeling $C_n\odot P_2$

Input: *Img* (Digital Image)
Output: *Adj Matrix* (Adjacency Matrix)

1. Input Img
2. Define Img size as row and column
3. **if** *row* > *column* **then**
4. n = $\left\lceil\frac{row}{3}\right\rceil$
5. *Define k value*
6. *Elements of Adj Matrix*
7. **else if** *row* < *column* **then**
8. n = $\left\lceil\frac{column}{3}\right\rceil$
9. *Define k value*
10. *Elements of Adj Matrix*

Algorithm 2: Image Encryption Algorithm

Input: *PlainImg* (Digital Image), *Adj Matrix* (Adjacency Matrix), *k*
Output: CipherImg (Image Encryption Results)

Input *PlainImg*
Defined *PlainImg* size as row and column
a = *max* (*row, column*)
for *i* = *1*:*5*: *a* **do**
    [ERO*Img* = Elementary Row Operation on *PlainImg*
for *i*=*1*:*5*: *a* **do**
    [Key = Elementary Row Operation on Adj Matrix
CipherImg = (ERO *Img* + Key) *mod* 255

Algorithm of Keystream

In this section, we will show you an important method in data encryption, the keystream algorithm. This algorithm is responsible for generating the key sequence used in the encryption process. By understanding the keystream algorithm, we can design a reliable data security system with keys that are difficult for unauthorized parties to guess. The keystream algorithm can be seen in Algorithm 1.

Algorithm of Encryption Process

In this section, we will show you another important method of data encryption, the encryption algorithm. This algorithm plays an important role in keeping sensitive information confidential. The algorithm of the encryption process can be seen in Algorithm 2.

Discussion

Figure (2) shows the framework proposed cryptosystem. On that figure, the process begins by reading the size of the plain image. This size is used as a reference to determine the size of the graph to be constructed. The graph is then converted into an adjacency matrix representation, which contains pairs of adjacent nodes. We also convert the plain image into a matrix that contains pixel intensity values. After obtaining the matrices, we can perform mathematical operations. The mathematical operation we use is Elementary Row Operations (ERO). This operation allows us to randomize the matrix values, resulting in a blurred encryption (cipher image). There are two matrices we operate on using ERO: The adjacency matrix and the pixel matrix. After applying ERO to each matrix, we then use the Caesar cipher technique to sum the two matrices. The sum is then taken modulo 255, as 255 is the maximum intensity of a pixel.

We use seven theorems from different graphs to construct the keystream. In the Vertex Irregular Reflexive Graph, we take Helmet (H_n), Split Star (SS), and Complete (K_2, n). While on the Edge Irregular Reflexive Graph we take Broom ($Br_{n,m}$), Double Star ($DS_{m,n}$), Ladder (L_n), and $Cn \odot P_2$. We analyze the cipher image based on four parameters: Correlation analysis, Number of Pixels Change Rate (NPCR) value analysis, Unified Average Changing Intensity (UACI) value analysis, and Peak Signal Noise Ratio (PSNR) value analysis. Correlation analysis aims to measure the degree of correlation between the pixels of the plain image and the cipher image. The correlation value ranges from negative, indicating no correlation, to positive, indicating a correlation. The more random the cipher image is, the more negative the correlation value will be. The Number of Pixels Change Rate (NPCR) value gives an idea of how much change has occurred after we encrypt the image. The greater the NPCR value, the more pixels will change during the encryption process. Unified Average Changing Intensity (UACI) provides an overview to evaluate the quality of the cipher image. The greater the Unified Average Changing Intensity (UACI) value, the greater the change in intensity that occurs in the image pixels during the encryption process. Peak Signal Noise Ratio (PSNR) can provide an overview to evaluate the similarity between the plain image and the cipher image. The smaller Peak Signal to Noise Ratio (PSNR) value indicates the dissimilarity between the plain image and the cipher image.

Next, we will compare the results of the iris data encryption process using edge irregular reflexive labeling and vertex irregular reflexive labeling. The comparison results can be seen in the relevant table. The iris is a unique part of the human body that can be used to identify a person with a high degree of accuracy. However, due to its uniqueness, information about the iris is very sensitive and vulnerable to misuse if not properly protected. Therefore, the encryption algorithm must make the iris image difficult to recognize. The included table shows the encryption results on iris images using various irregular reflexive labeling on different graphs.

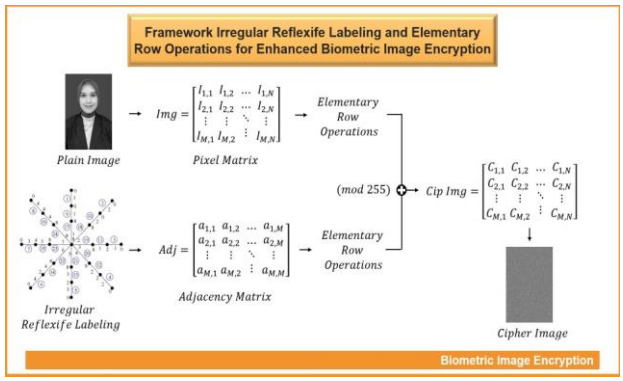

Fig. 2: Framework proposed cryptosystem

In general, the encryption results using all graphs as encryption keys have shown high encryption accuracy. This can be seen from the low correlation values, which indicate that there is no clear relationship or pattern between the original image and the encrypted image. In this context, low correlation indicates a high level of randomness in the encrypted image, which is a highly desirable property in information security. When the correlation between the original image and the encrypted image is low, unauthorized parties will have difficulty obtaining information or finding patterns in the encrypted image without knowing the encryption key used. This makes the encrypted image more secure and enhances the confidentiality of the encrypted data. The Subdivided Star graph has the lowest correlation value among the other graphs with Vertex Irregular labeling. Another graph, $C_n \odot P_2$, shows the lowest correlation value with edge irregular labeling.

The next analysis based on NPCR values shows that the Helm graph has the highest NPCR value among the graphs with vertex irregular labeling. A high NPCR value indicates a high degree of pixel change between the original image and the encrypted image, making it difficult for unauthorized parties to reconstruct the original image from the encrypted image. The $C_n \odot P_2$ graph shows the highest NPCR value among the graphs with edge irregular labeling.

The UACI analysis shows that the Subdivided Star graph has the highest UACI value among the graphs with vertex irregular labeling. A high UACI value indicates significant changes in pixel intensity between the original image and the encrypted image, making it difficult for unauthorized parties to reconstruct the original image from the encrypted image. The $C_n \odot P_2$ graph has the highest UACI value among the graphs with edge irregular labeling.

The final analysis based on PSNR values shows that the Helm graph has the highest PSNR value among the graphs with vertex irregular labeling. A high PSNR value indicates a high level of similarity between the original image and the encrypted image, thus increasing confidence in the success of the encryption process. The $C_n \odot P_2$ graph has the lowest PSNR value among the graphs with edge irregular labeling.

Based on these four analyses, the shape of the graph affects the encryption results. This can be seen from the different values of correlation, NPCR, UACI, and PSNR for each graph. The $C_n \odot P_2$ graph shows the best results in the edge irregular labeling type compared to other graphs. Therefore, it can be concluded that the $C_n \odot P_2$ graph with edge irregular labeling is the best graph for iris data encryption among the other graphs.

Biometric data, such as facial images, is highly sensitive personal information that must be protected to prevent unauthorized access. Facial image encryption helps enhance the security of sensitive biometric data. By using facial image encryption, the speed and efficiency of the biometric recognition process can be improved. Even when facial data is encrypted, facial recognition algorithms can still quickly and accurately identify unique facial patterns. Table (2) shows the encryption results on facial images using various irregular reflexive labelings on different graphs.

Next, we will analyze the values in the table. The first analysis is the correlation value in the facial image encryption results. The complete graph has the lowest correlation value among the graphs with Vertex Irregular labeling. The $C_n \odot P_2$ and ladder graphs also have the lowest correlation values among the graphs with edge irregular labeling.

The second analysis is the NPCR value. The complete graph shows the highest NPCR value among the graphs with vertex irregular labeling. The ladder graph has the highest NPCR value among the graphs with edge irregular labeling. A high NPCR indicates a significant level of pixel change between the original image and the encrypted image, making it difficult for unauthorized parties to reconstruct the original image from the encrypted image.

The third analysis is the UACI value. The complete graph has the highest UACI value among the graphs with vertex irregular labeling. The Double Star graph has the highest UACI value among the graphs with edge irregular labeling. A high UACI indicates significant changes in pixel intensity between the original image and the encrypted image, making it more difficult for unauthorized parties to reconstruct the original image.

Table 2: Iris Image encryption results

Name graph	Types labeling	Correlation	Iris Image NPCR	UACI	PSNR
Complete	Vertex	0.0064	99.5146	26.0091	7.7935
Subdivided star	Vertex	-7.32×10^{-4}	99.5742	26.0352	7.7922
Helm	Vertex	-5.02×10^{-4}	99.5768	26.0350	7.7927
$Cn \odot P2$	Edge	-8.26×10^{-5}	99.6833	26.5277	7.7208
Broom	Edge	−0.0014	99.5755	26.0431	7.7902
Double star	Edge	-6.95×10^{-4}	99.5794	26.0329	7.7917
Ladder	Edge	-5.42×10^{-4}	99.5729	26.0317	7.7930
AES		−0.00206	99.6132	26.2250	7.8998
DES		−0.00516	99.6276	25.6431	7.8830

The final analysis is based on the PSNR value. The complete graph has the lowest PSNR value among the graphs with vertex irregular labeling. The $C_n \odot P_2$ and Double Star graphs have the lowest PSNR values among the graphs with edge irregular labeling. A low PSNR value indicates that the encrypted image has significant differences from the original image, thereby increasing confidence in the success of the encryption process.

Based on the analysis results, the best values for correlation, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Peak Signal to Noise Ratio (PSNR) for the iris image were obtained using the complete graph. The elements in the adjacency matrix of the complete graph are more fully populated compared to the adjacency matrices of other graphs. Consequently, many matrix elements can be manipulated during the encryption process. This leads to better encryption results because the encryption method we use operates simultaneously between the keystream and the original image using elementary row operations. In this operation, if many populated elements are swapped and manipulated, it can result in non-zero values, thus making the encryption results more random.

The next analysis is the encryption results of fingerprint images. Encrypting fingerprint images is crucial for protecting the security and privacy of sensitive data. Fingerprint images are frequently used in various identification applications, including device security, financial transaction authorization, and access control. By applying encryption to fingerprint images, sensitive biometric information can be secured against unauthorized access or identity theft. This ensures that only authorized users can access and utilize the fingerprint data while protecting individual privacy and security. Table (3) shows the encryption results of fingerprint images using various irregular reflexive labelings on different graphs.

Next, we will analyze the values in the table. The first analysis is the correlation value. The complete graph has the lowest correlation value among the graphs with vertex correlation value among the graphs with edge irregular labeling. The $C_n \odot P_2$ graph also has the lowest labeling. A low correlation value indicates that there is no clear relationship between the original image and the encrypted image, which is a desirable property in information security.

The second analysis is the NPCR value. The complete graph shows the highest NPCR value among the graphs with vertex irregular labeling. The ladder graph has the highest NPCR value among the graphs with edge irregular labeling. A high NPCR value indicates a high degree of pixel change between the original image and the encrypted image, making it difficult for unauthorized parties to reconstruct the original image from the encrypted image.

The third analysis is the UACI value. The complete graph has the highest UACI value among the graphs with vertex irregular labeling. The $C_n \odot P_2$ graph has the highest UACI value among the graphs with edge irregular labeling. A high UACI value indicates significant changes in pixel intensity between the original image and the encrypted image, increasing the difficulty for unauthorized parties to reconstruct the original image.

The final analysis is based on the PSNR value. The complete graph has the lowest PSNR value among the graphs with vertex irregular labeling. The $C_n \odot P_2$ graph has the lowest PSNR value among the graphs with edge irregular labeling. A low PSNR value indicates that the encrypted image has significant differences from the original image, thus increasing confidence in the success of the encryption process.

Based on the results of these four analyses, the complete graph shows the best results for correlation, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Peak Signal to Noise Ratio (PSNR) for fingerprint images. The elements in the adjacency matrix are more fully populated compared to other graphs, allowing more matrix elements to be manipulated during the encryption process. This results in better encryption outcomes because the encryption method used operates simultaneously between the keystream and the original image using elementary row operations. When many filled elements are swapped and manipulated in this operation, it generates non-zero values, making the encryption results more random and secure.

Table 3: Face image encryption results

Name graph	Types labeling	Correlation	Face image NPCR	UACI	PSNR
Complete	Vertex	-8.33×10^{-4}	99.6070	7.4650	7.6632
Subdivided star	Vertex	−0.003	99.6045	7.2589	7.9662
Helm	Vertex	−0.0029	99.6037	7.2588	7.9673
$Cn\odot P2$	Edge	−0.0029	99.6040	7.2579	7.9658
Broom	Edge	−0.0030	99.6041	7.2587	7.7969
Double star	Edge	−0.0031	99.6040	7.2592	7.9658
Ladder	Edge	−0.0029	99.605	7.2577	7.9660
AES		−0.0244	99.6059	7.4650	7.6996
DES		−0.0305	99.7466	7.2946	8.857

DOI: 10.3844/jcssp.2024.1766.1777

Next, we will perform a comparative analysis of the seven theorems with the results of other studies, specifically those using AES and DES. The comparison results can be seen in Fig. (3). The comparison shows that encryption using vertex irregular reflexive labeling from the complete graph produces the best cipher image. This is due to several key factors.

First, the vertex irregular reflexive labeling method on the complete graph shows a very low correlation value between the original image and the encrypted image. This indicates that the patterns in the original image cannot be easily recognized in the encrypted image, enhancing data security.

Second, the high values of the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) indicate that this method results in significant changes in the pixel level and image intensity, making it very difficult to reconstruct the original image from the encrypted image. This provides an advantage over AES and DES, which may not achieve the same level of pixel and intensity changes.

Third, the lower Peak Signal to Noise Ratio (PSNR) value indicates that the encrypted image is significantly different from the original image, which is a sign of success in hiding the original information from unauthorized parties.

Overall, the combination of low correlation values, high NPCR and UACI values, and low PSNR values makes the vertex irregular reflexive labeling method on the complete graph superior to AES and DES in terms of security and effectiveness in encrypting biometric images. Thus, this method should be considered a more effective solution for protecting sensitive data.

Additionally, we analyzed the results of the image encryption process using histogram analysis. Histogram analysis of the encrypted image is a method to visualize the distribution of pixel intensity in the encrypted image. This analysis helps evaluate the level of randomness and uniformity in the encrypted image, which is crucial for assessing the effectiveness of the encryption process in altering the original structure of the image. A more uniform distribution of pixel intensities in the histogram indicates a higher level of security, as it makes it more difficult for unauthorized parties to extract information from the encrypted image. Therefore, histogram analysis becomes an essential step in validating the security of the encryption algorithm used.

Next, we discuss the histogram analysis of the encrypted image compared to the original image. In the original image, pixel intensity values range from 1 to 255, with a concentration around 50, indicating a tendency towards brighter colors. Conversely, the histogram of the encrypted image shows a uniform and dense distribution of pixel intensities across the entire range. This uniformity and randomness in the histogram indicate that the encryption process effectively disguises the original image, making it visually unrecognizable. The results of this histogram comparison are shown in Fig. (4), which demonstrates an even and random spread of pixel intensities.

A good histogram in the encrypted image indicates that the encryption process has successfully concealed the original information, making it difficult for unauthorized parties to reconstruct or access the data. The absence of visible patterns or identifiable information in the histogram enhances the security and integrity of the encrypted data. Thus, a well-distributed histogram is a key indicator of the encryption algorithm's effectiveness in maintaining data confidentiality.

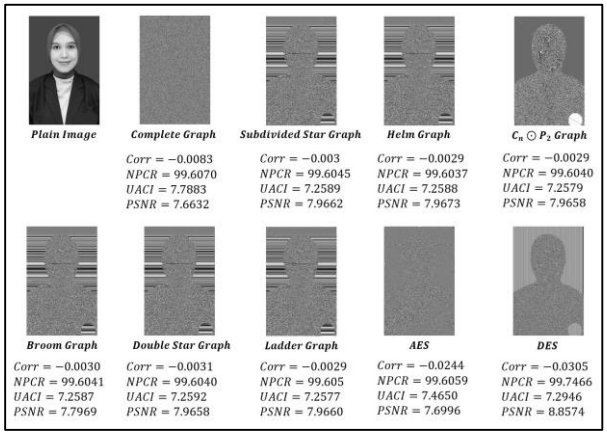

Fig. 3: The comparison of our methods

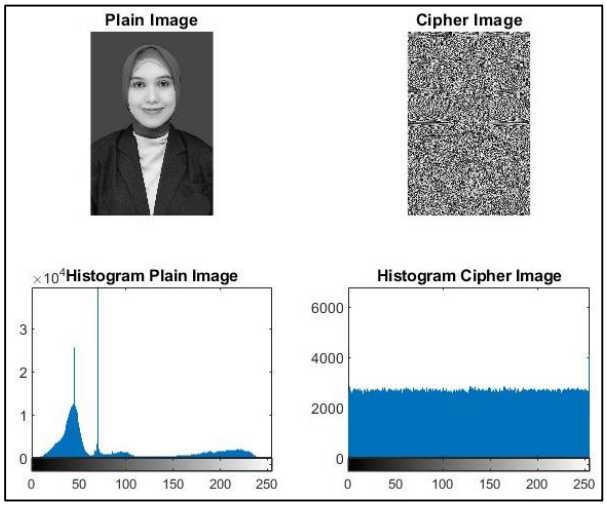

Fig. 4: The histogram comparison between plain image and cipher image

Table 4: Fingerprint image encryption results

Name graph	Types Labeling	Correlation	Fingerprint Image NPCR	UACI	PSNR
Complete	Vertex	−0.0035	99.5447	32.9100	5.7000
Subdivided star	Vertex	−0.0013	98.7162	32.4450	5.7154
Helm	Vertex	−0.0012	98.7207	32.4310	5.7167
$Cn \odot P2$	Edge	−0.0035	98.7177	32.4870	5.7052
Broom	Edge	−0.0027	98.7230	32.4431	5.7115
Double star	Edge	−0.0019	98.7220	32.4525	5.7120
Ladder	Edge	−0.0027	98.7260	32.4487	5.7127
AES		−0.00161	99.2237	32.6190	5.6914
DES		0.02805	98.9326	31.5016	7.8769

Our proposed encryption method has been shown to outperform the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) (More *et al*., 2021). Tables (3-4) show that our proposed method has outperformed AES and DES in terms of correlation, UACI, NPCR, and PSNR. This indicates that our proposed method provides a higher level of security and is resistant to cryptographic attacks. It can be a superior option to protect data from increasingly sophisticated security threats.

Conclusion

In this study, we propose a cryptosystem method that uses irregular reflexive labeling and encryption based on elementary row operations to improve the security of biometric images. Our approach introduces a novel combination of edge and vertex irregular reflexive *k*-labeling with row elementary operations, which to our knowledge, has not been explored in existing encryption techniques. This novel combination enhances the security of the encryption process by making the resulting keystreams more robust against attacks.

Through our tests, we found that providing irregular reflexive labeling as a keystream has a significant effect on improving security. This can be seen from the correlation test, NPCR test, UACI test, and PSNR test, which we document in Tables (3-4). Our proposed encryption scheme shows superior performance compared to AES and DES in terms of correlation, PSNR, NPCR, and UACI.

In addition, we discovered that complete graphs, especially in the context of the irregular reflexive labeling theorem, provide optimal results in generating high-quality keystreams for face and fingerprint image encryption. In contrast, the $C_n \odot P_2$ graph, within the framework of the irregular edge labeling theorem, yields optimal results for iris image encryption.

However, the effectiveness of this cryptosystem method varies depending on the type of graph used. This variation indicates that there are still open questions regarding the efficacy of other graph types in producing high-quality encryption. These findings highlight the potential for future research to explore other graph structures and their impact on encryption performance. Thus, our contribution not only offers a novel and effective method for biometric image encryption but also provides valuable insights for the future development of biometric security technology, suggesting new directions for further enhancing the robustness and security of encryption techniques.

Acknowledgment

We gratefully acknowledge PUI-PT Combinatoric and Graph, CGANT-Universitas Jember, for providing supervision, suggestions, and collaboration in finishing this study. We also would like to thank LP2M-Universitas Jember and DRTPM for the research support for the year 2024.

Funding Information

The authors received financial support from PUI-PT Combinatoric and Graph, CGANT-Universitas Jember; LP2M-Universitas Jember, and DRTPM.

Author's Contributions

Ika Hesti Agustin: Analyzed Irregular Reflexife Labeling, developed the methodology, and designed the proposed method.

Dafik: Analyzed Irregular Reflexife Labeling, designed the proposed method, and developed an algorithm.

Rifki Ilham Baihaki: Developed an algorithm and programming, conducted experimental testing, and contributed to results interpretation.

Marsidi: Analyzed Irregular Reflexife Labeling and developed the methodology.

Kiswara Agung Santoso: Conducted data collection, assisted in the analysis, and contributed to results interpretation.

Ethics

The authors confirm that this manuscript has not been published elsewhere and that no ethical issues are

involved because the article conforms to all scientifically known ethical principles.

References

Agustin, I. H., Dafik, Imam Utoyo, M., Slamin, & Venkatachalam, M. (2021). The Reflexive Edge Strength on Some Almost Regular Graphs. *Heliyon*, *7*(5), e06991. https://doi.org/10.1016/j.heliyon.2021.e06991

Agustin, I. H., Utoyo, M. I., Dafik, & Venkatachalam, M. (2021). The Vertex Irregular Reflexive Labeling of Some Almost Regular Graph. *Palestine Journal of Mathematics*, *10*(2), 83–91. https://doi.org/10.1080/097205292022.2063543

Agustin, I. H., Susilowati, L., Dafik, Cangul, I. N., & Mohanapriya, N. (2022). On the Vertex Irregular Reflexive Labeling of Several Regular and Regular-Like Graphs. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(5), 1457–1473. https://doi.org/10.1080/09720529.2022.2063543

Agustin, I. H., Utoyo, M. I., Dafik, D., Venkatachalam, M., & Supangken, S. (2020). On the Construction of the Reflexive Vertex -Labeling of Any Graph with Pendant Vertex. *International Journal of Mathematics and Mathematical Sciences*, *2020*, 1–8. https://doi.org/10.1155/2020/7812812

Agustin, I. H., Utoyo, M. I., Dafik, Mohanapriya, N., & Slamin. (2023). The Reflexive Vertex Strength on Cycle and Generalized Friendship Graph. *Asian-European Journal of Mathematics*, *16*(8), 2350137. https://doi.org/10.1142/s1793557123501371

Ahmad, A., Al-Mushayt, O. B. S., & Bača, M. (2014). On edge irregularity strength of graphs. *Applied mathematics and computation*, *243*, 607-610. https://doi.org/10.1016/j.amc.2014.06.028

Ahmad, M., Agarwal, S., Alkhayyat, A., Alhudhaif, A., Alenezi, F., Zahid, A. H., & Aljehane, N. O. (2022). An Image Encryption Algorithm Based on New Generalized Fusion Fractal Structure. *Information Sciences*, *592*, 1–20. https://doi.org/10.1016/j.ins.2022.01.042

Alfarisi, R., Ryan, J., Siddiqui, M. K., Dafik, & Agustin, I. H. (2021). Vertex Irregular Reflexive Labeling of Disjoint Union of Gear and Book Graphs. *Asian-European Journal of Mathematics*, *14*(5), 2150078. https://doi.org/10.1142/s1793557121500789

Bača, M., Irfan, M., Ryan, J., Semaničová-Feňovčíková, A., & Tanna, D. (2019). Note on edge irregular reflexive labelings of graphs. *AKCE International Journal of Graphs and Combinatorics*, *16*(2), 145-157. https://doi.org/10.1016/j.akcej.2018.01.013

Bača, M., Miller, M., & Ryan, J. (2007). On irregular total labellings. *Discrete mathematics*, *307*(11-12), 1378-1388. https://doi.org/10.1016/j.disc.2005.11.075

Bača, M., Irfan, M., Ryan, J., Semaničová-Feňovčíková, A., & Tanna, D. (2017). On edge irregular reflexive labellings for the generalized friendship graphs. *Mathematics*, *5*(4), 67. https://doi.org/10.3390/math5040067

Chartrand, G., Erdös, P., & Oellermann, O. R. (1988). How to define an irregular graph. *The College Mathematics Journal*, *19*(1), 36-42. https://doi.org/10.2307/2686701

Gallian, J. A. (2022). A Dynamic Survey of Graph Labeling. *The Electronic Journal of Combinatorics*, *6*(25), 4–623. https://doi.org/10.37236/11668

Guirao, J. L. G., Ahmad, S., Siddiqui, M. K., & Ibrahim, M. (2018). Edge Irregular Reflexive Labeling for Disjoint Union of Generalized Petersen Graph. *Mathematics*, *6*(12), 304. https://doi.org/10.3390/math6120304

Ibrahim, M., Majeed, S., & Siddiqui, M. K. (2020). Edge Irregular Reflexive Labeling for Star, Double Star, and Caterpillar Graphs. *TWMS Journal of Applied and Engineering Mathematics*, *10*(3), 718–726. https://doi.org/10.3390/math6120304

Indriati, D., Widodo, & Rosyida, I. (2020). Edge Irregular Reflexive Labeling on Corona of Path and Other Graphs. *Journal of Physics: Conference Series*, 012004. https://doi.org/10.1088/1742-6596/1489/1/012004

Kairess. (2022). *Fingerprint Recognition*. https://www.kaggle.com/code/kairess/ fingerprint-recognition/input

Maryati, T. K., Atiqoh, K. S. N., Nisviasari, R., Agustin, I. H., Dafik, & Venkatachalam, M. (2020). The Construction of Block Cipher Encryption Key by Using a Local Super Antimagic Total Face Coloring. *Advances in Mathematics: Scientific Journal*, *9*(3), 1349–1362. https://doi.org/10.37418/amsj.9.3.59

Marzuki, C. C., Salman, A. N. M., & Miller, M. (2013). On the total Irregularity Strength of Cycles and Paths. *Far East Journal of Mathematical Sciences*, *82*(1), 1. https://doi.org/10.36478/rjasci.2018.582.586

Mohammad, N. (2024). *MMU Iris Dataset*. www.kaggle.com/datasets/naureenmohammad/mmu-iris-dataset

More, S. S., Narain, B., & Jadhav, B. T. (2021). Advanced Encryption Standard Algorithm in Multimodal Biometric Image. In A. A. Rizvanov, B. K. Singh, & P. Ganasala (Eds.), *Advances in Biomedical Engineering and Technology* (pp. 53–66). Springer. https://doi.org/10.1007/978-981-15-6329-4_7

Putra, R. W., & Susanti, Y. (2018). On Total Edge Irregularity Strength of Centralized Uniform Theta Graphs. *AKCE International Journal of Graphs and Combinatorics*, *15*(1), 7–13. https://doi.org/10.1016/j.akcej.2018.02.002

Prihandoko, A. C., Dafik, D., & Agustin, I. H. (2022). Stream-Keys Generation Based on Graph Labeling for Strengthening Vigenere Encryption. *International Journal of Electrical and Computer Engineering (IJECE)*, *12*(4), 3960–3969. https://doi.org/10.11591/ijece.v12i4.pp3960-3969

Ratnasari, L., & Susanti, Y. (2020). Total Edge Irregularity Strength of Ladder-Related Graphs. *Asian-European Journal of Mathematics*, *13*(4), 2050072. https://doi.org/10.1142/s1793557120500722

Su, J., Sun, H., Wang, H., & Yao, B. (2020). Topological Public-Key Cryptography Based On Graph Image-Labellings for Information Security. *2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*, 366–370. https://doi.org/10.1109/iciba50161.2020.9277154

Susanti, Y., Puspitasari, Y. I., & Khotimah, H. (2020). On Total Edge Irregularity Strength of Staircase Graphs and Related Graphs. *Iranian Journal of Mathematical Sciences and Informatics*, *15*(1), 1–13. https://doi.org/10.29252/ijmsi.15.1.1

Tanna, D., Ryan, J., Semaničová-Feňovčíková, A., & Bača, M. (2020). Vertex Irregular Reflexive Labeling of Prisms and Wheels. *AKCE International Journal of Graphs and Combinatorics*, *17*(1), 51–59. https://doi.org/10.1016/j.akcej.2018.08.004

Tarawneh, I., Hasni, R., & Asim, M. A. (2018). On the Edge Irregularity Strength of Disjoint Union of Star Graph and Subdivision of Star Graph. *Ars Comb*, *141*, 93–100.

Tarawneh, I., Hasni, R., Ahmad, A., Lau, G.-C., & Lee, S.-M. (2020). On the Edge Irregularity Strength of Corona Product of Graphs with Cycle. *Discrete Mathematics, Algorithms and Applications*, *12*(6), 2050083. https://doi.org/10.1142/s1793830920500834

Wen, H., Zhang, C., Chen, P., Chen, R., Xu, J., Liao, Y., Liang, Z., Shen, D., Zhou, L., & Ke, J. (2021). A Quantum Chaotic Image Cryptosystem and its Application in IoT Secure Communication. *IEEE Access*, *9*, 20481–20492. https://doi.org/10.1109/access.2021.3054952

Yongsheng, K., Muhammad Javed Azhar, K., Muhammad, I., & Muhammad Kamran, S. (2021). On Edge Irregular Reflexive Labeling for Cartesian Product of Two Graphs. *The European Physical Journal Plus*, *136*(1), 6. https://doi.org/10.1140/epjp/s13360-020-00960-1

Yoong, K.-K., Hasni, R., Irfan, M., Taraweh, I., Ahmad, A., & Lee, S.-M. (2021). On the Edge Irregular Reflexive Labeling of Corona Product of Graphs with Path. *AKCE International Journal of Graphs and Combinatorics*, *18*(1), 53–59. https://doi.org/10.1080/09728600.2021.1931555

Zhang, X., Ibrahim, M., Bokhary, S. A. ul H., & Siddiqui, M. K. (2018). Edge Irregular Reflexive Labeling for the Disjoint Union of Gear Graphs and Prism Graphs. *Mathematics*, *6*(9), 142. https://doi.org/10.3390/math6090142