بسم الله الرحمن الرحيم

Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security

Ijaz Khalid

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan

2023

Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security

Ijaz khalid

Supervised by

Prof. Dr. Tariq Shah

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan

2023

Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security

A Thesis Submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad, in the partial fulfillment of the requirement for the degree of

Doctor of Philosophy

in

Mathematics

By

Ijaz Khalid

Supervised by

Prof. Dr. Tariq Shah
Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2023

Author's Declaration

I, **Ijaz Khalid,** hereby state that my PhD thesis titled **Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security** is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the university has the right to withdraw my PhD degree.

Name of Student: **Ijaz Khalid**

Date: **31-Aug-2023**

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and **Quaid-i-Azam University** towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Student/Author Signature

Name: **Ijaz Khalid**

Certificate of Approval

This is to certify that the research work presented in this thesis entitled **Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security** was conducted by **Mr. Ijaz Khalid** under the kind supervision of **Prof. Dr. Tariq Shah**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in field of Mathematics from Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan.

Student Name: **Ijaz Khalid** Signature:__________

External committee:

a) **External Examiner 1**: Signature: Akbar Azam
Name: **Dr. Akbar Azam**
Designation: Professor
Office Address: Department of Mathematics, COMSATS University, Park Road, Chak Shahzad, Islamabad.

b) **External Examiner 2**: Signature:__________
Name: **Dr. Matloob Anwar**
Designation: Professor
Office Address: School of Natural Sciences (SNS), National University of Sciences and Technology, NUST, H-12, Islamabad.

c) **Internal Examiner** Signature: Tariq Shah
Name: **Prof. Dr. Tariq Shah**
Designation: Professor
Office Address: Department of Mathematics, QAU Islamabad.

Supervisor Name: Signature: Tariq Shah
Prof. Dr. Tariq Shah

Name of Dean/ HOD Signature: Tariq Shah

Prof. Dr. Tariq Shah

Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security

By

Ijaz Khalid

CERTIFICATE

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF THE

DOCTOR OF PHILOSOPHY IN MATHEMATICS

We accept this thesis as conforming to the required standard

1. Tariq Shah

Prof. Dr. Tariq Shah
(Chairman)

2. Tariq Shah

Prof. Dr. Tariq Shah
(Supervisor)

3. ______________________

Prof. Dr. Akbar Azam
(External Examiner)

Department of Mathematics, COMSATS University, Park Road, Chak Shahzad, Islamabad.

4. ______________________

Prof. Dr. Matloob Anwar
(External Examiner)

School of Natural Sciences (SNS), National University of Sciences and Technology, NUST, H-12, Islamabad.

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2023

Dedicate to

My Beloved Wife, Mahnoor Ijaz and Children, Hoorain Fatima and Muhammad Arham

Acknowledgement

All praise for almighty Allah, the creator and the Merciful Lord, who guides me in darkness, helps me in difficulties and enables me to reach the ultimate stage with courage. All of my reverence and devotion goes to our beloved Prophet Muhammad, peace be upon him, the source of humanity, kindness and guidance for the whole creatures, who declared it an obligatory duty of every Muslim to seek and acquire knowledge.

I would like to take this opportunity to express my deepest gratitude to kind-hearted Prof. Dr Tariq Shah, who is my first supervisor; for the great opportunity he provided me to pursue a Doctoral degree; for his expertise in the area that has guided me throughout the study; and for his advice, inspiration and constant encouragement to complete this degree.

I extended my thanks to those participants who gave their valuable time, great effort and enthusiasm to participate in the pilot and the main study. They also provided helpful comments and insights on the issue studied. Again, my sincere appreciation goes to them for their collective thoughts and experiences.

Furthermore, I appreciate Quaid-i-Azam University Islamabad Pakistan, who generously helped me by approving the scholarship to make this Doctoral study possible.

In addition, I also thank my research fellows and friends, Asst. Prof. Muhammad Imran Haider, Dr Dawood Shah, Dr Muhammad Asif, Dr Atta Ullah, Dr Tanveer Ul Haq, Muhammad Hussain, Aftab Akram and Mahnoor for giving their valuable suggestions. Not only these Mathematicians of Quaid-i-Azam University but also thanks to my friends Muhammad Awais, Adil Siddique, Muhammad Asif, Muhammad Afaq Khan, Baber Zaman, Umair Hassan, Hayat Khan, Ummi Habiba, Rimsha and sweet Ayesha, who refreshed me during the journey of my PhD.

My utmost special thanks go to the most important and essential people in my life, my family, for their love, prayers, courage and moral support throughout the study. They are my beloved parents, lovely wife, children, and loving siblings. Thank you for being there for me. Finally, I acknowledged the support from everyone in the Quaid-i-Azam University Department of Mathematics. Please accept my gratitude now and always.

Ijaz Khalid

16-Jan-2023

Preface

Due to the rapid advancement of science and digital technology, the importance of digital data in everyday life has grown tremendously over the past several decades. Nowadays, digital data are employed in many spheres of life, including commerce, military image databases, private video conferences, finance, engineering, mathematics, the arts, advertising, healthcare and scientific research. Digital data processing tools and digital documentation are becoming increasingly important due to the expanded significance of digital data in the age of information technology. Consequently, it has improved digital data transmission over the public channel. Since the internet network is widely accessible, it has generated plausible opportunities that endanger the integrity and confidentiality of digital data during dissemination over the internet. Cryptography is the study of information security strategies used to combat these threats.

Over the past 60 years, cryptography has gained recognition as a legitimate scientific field. However, comparatively, it is an entirely new and faster-growing study area compared to other science areas, and each moment carries continual developments. The field of cryptography is divided mainly into two sub-branches: a) Symmetric Cryptography and b) Asymmetric Cryptography. This classification of cryptography is based on the input key and confidential data used for encryption and decryption. In symmetric-key cryptography, the communication parties secretly share a private key. The Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest Cipher 4 (RC4), International Data Encryption Algorithm (IDEA), Serpent, TwoFish, Camellia, SM4 and Lucifer are some well-known symmetric key cryptography algorithms. AES-128, AES-192, and AES-256 are the most often used symmetric algorithms. From the resource utilization point of view, the symmetric key algorithms require few resources to operate. Although owing to the usage of a single key for encryption, the symmetric algorithm is less secure. In symmetric-key cryptography, the communicating parties utilize the same private key for encryption and decryption. Thus, the security risks of sharing secret keys make public-key cryptography even more crucial. Public key cryptography employs a pair of distinct keys (private, public) for encryption and decryption and is much safer as two keys are involved. The primary goal of public key cryptography, the cipher, is to protect the data from eavesdroppers even when they know the encryption key. Algorithms such as RSA, Elliptic Curve Cryptography(ECC), NTRU, Diffie-Hellman, Elgamal and McEliece are the most well-known public examples of asymmetric key cryptography.

Elliptic curve cryptography (ECC), which employs a pair of public-private keys, is the most prominent and well-known public-key cryptosystem. The concept has been used since the 19th century and has provided optimal solutions for many hard mathematical problems in literature, like the Fast Integers Factorization Problem (FIFP), searching for congruent numbers (SCN), etc. Nowadays, this concept is being extensively used in cryptographic applications. Principally, the use of these curves relies on the very existence of group law, making this a relatively good algorithm for the public key cryptosystem because the discrete logarithm problem is a hard problem relative to the size of the parameters used. Such curves also find application in digital signatures, bilinear pairing, and digital signatures. Being an alternative to the well-known RSA algorithm, elliptic curve cryptography offers better security with a much smaller key size than RSA and finite field discrete logarithm-based systems. Finite field Diffie-Hellman cryptosystems are known to be slow and susceptible to the number field sieve attack using precomputation, two limitations that do not apply to elliptic curves, as far as is currently known. Elliptic curve cryptosystems offer efficiency and security advantage over these systems. Until now, there hasn't been a more effective general attack for elliptic curves over prime fields with a subgroup of huge prime order than the exponentially fast Pollard's rho attack. Because of this security aspect, elliptic curve systems require a much smaller key size to offer the same level of security compared to Diffie Hellman and RSA. Moreover, the efficiency advantage makes them ideal for resource-constraint devices like smart cards and web servers where public key cryptography is a bottleneck. As a result, many organizations have encouraged the use of elliptic curves by proposing sets of suggested elliptic curves and algorithms on top of them, including the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and l'Agence Nationale de la Securité des Systemes d'Information (ANSSI).

The primary and most often utilized operation in elliptic curve cryptography is the scalar multiplication KP, where K is a private integer value that has to be secured where P is the point on an elliptic curve. The scalar multiplication of the elliptic curve is utilized in various cryptographic algorithms, including enciphering/deciphering of the data, the key generation process, and the digital signature signing and verification methods. Scalar, point, and field arithmetic are the three arithmetic levels implied by the mathematics of an elliptic curve. Many works are devoted to pointing arithmetic and scalar arithmetic to make a quick calculation of scalar multiplication, which is the main computation involved in ECC. Point arithmetic means the addition and successive doubling of the point of EC.

Elliptic curve cryptography has been widely used as a discrete mathematical structure in computer hardware and software. Finite fields EC are a beneficial structure with many uses in computer science and cryptography. One of the characteristics of finite filed curves is that they are typically executed more quickly on general-purpose CPUs because they usually include a big integer multiplier circuit instead of a big binary multiplier circuit. Furthermore, finite field curve efficiently implements hardware, prompting researchers to utilize it in cryptography. The reduction of cost and efficiency improvements are the main characteristics of EC over a finite field computation. In this thesis, we evaluate how the parameters of EC over a finite field affect the security features of symmetric, asymmetric and hybrid cryptographic techniques. The objective is to enhance the parameters of EC over a finite field and investigate how this will increase the security of the cryptosystems.

The thesis encompasses a total of six chapters. The fundamental concepts and mathematical background of EC are covered in the first chapter of this thesis. Furthermore, the main objective of this chapter is to provide a concise overview of the underlying concepts for EC-based cryptographic applications. In the subsequent chapters, these definitions and attributes are applied. The chapter also introduces the generalization of EC called hyperelliptic curve (HEC), which will be utilized in chapter four for watermarking encryption scheme. The chapter concludes with the complexity theory.

The second chapter of this thesis introduces a hybrid architecture named an integrated encryption scheme for multimedia data security. In the hybrid architecture approach, the data encoding and decoding approaches combined the efficiency of symmetric key encryption with the speed and convenience of an asymmetric key encryption scheme. The scheme introduced in this chapter is the enhanced version of the EC integrated encryption scheme (E-ECIES) over a finite field $\mathcal{F}_q$. This E-ECIES ensures confidentiality, user authentications, and secure key sharing among the communicating parties. Initially, the users share a secret parameter using Diffie-Hellman over the EC and pass it through SHA-256. Afterwards, the proposed scheme uses the first 128 bits for the confidentiality of the data, while the remaining 128-bits are for authentication. The confusion module is achieved by affine power affine transformation in the encryption algorithm. In contrast, the diffusion module is attained through highly nonlinear sequences generated through the EC.

The third chapter of this thesis introduced an efficient digital audio encryption algorithm with the design of a substitution permutation network (SPN) using a Mordell elliptic curve (MEC).

This newly designed scheme is based on the core mathematical operations of an EC over a finite prime field $\mathcal{F}_q$. As the rich mathematical operations of the EC are accomplished efficiently, a decent-quality sequence of Pseudo-random numbers is obtained in the initial module of the encryption procedure. After that, the plain audio data matrix is defused using these highly random sequences. Multiple 5×5 bijective S-boxes perform the confusion part of the scheme with optimal nonlinearity. The experimental findings support the proposed permutation-substitution architecture scheme's ability to defend against various attacks.

Chapter 4 of this thesis presents a novel digital watermarking scheme. In this era where the popularity and availability of the internet are at their peak, online storage devices are very easily accessible. The essay accessibility of online data has made the distribution, replication, and creation of digital data hassle-free. This problem led to the developing of a robust algorithm that could prevent copyright breaches. Therefore, this chapter presents a novel image watermarking scheme based on the hyperelliptic curve (HEC). The suggested scheme is key-dependent, and only the main owner of the image can prove his ownership using his secret key. The proposed scheme uses random sequences generated through the HEC and randomly distributes the watermark image's data. The random distribution of the watermark image, on the one hand, does not produce an effect on the quality of the host image; on the hand, this method enhances the security of the suggested watermarking technique, as only the authorized owner can reproduce the watermark image. Additionally, the chapter is concluded with the analytical findings of the proposed approach and a comparison to other current schemes.

Finally, in chapter 5, a symmetric key encryption algorithm was designed based on the efficient computation of elliptic curve isomorphism and small substitution boxes for the application of grayscale and binary image security. Since the data of plain images contain a high amount of correlated pixels, thus, the mere reliance on standard algorithms like AES, RSA, and DES is unsuitable for multimedia data security. Therefore, this chapter deliberates the efficient algorithms for multimedia data security. The suggested schemes are thoroughly evaluated against linear and differential attacks. The experimental findings of the proposed scheme show the efficiency of the system against different attacks.

The conclusion and a few ideas for potential future work are covered in the last chapter.

List of Publications

1. Khalid, I., Shah, T., Almarhabi, K. A., Shah, D., Asif, M., & Ashraf, M. U. (2022). The SPN network for digital audio data based on elliptic curve over a finite field. *IEEE Access*, *10*, 127939-127955.

2. Khalid, I., Shah, T., Eldin, S. M., Shah, D., Asif, M., & Saddique, I. (2022). An integrated image encryption scheme based on elliptic curve. *IEEE Access*, *11*, 5483-5501.

3. Shah, D., Shah, T., Ahamad, I., Haider, M. I., & Khalid, I. (2021). A three-dimensional chaotic map and their applications to digital audio security. *Multimedia Tools and Applications*, *80*, 22251-22273.

4. Khalid, I., Jamal, S. S., Shah, T., Shah, D., & Hazzazi, M. M. (2021). A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes. *IEEE Access*, *9*, 77798-77810.

5. Haider, M. I., Shah, T., Ali, A., Shah, D., & Khalid, I. (2023). An Innovative approach towards image encryption by using novel PRNs and S-boxes Modeling techniques. *Mathematics and Computers in Simulation*, *209*, 153-168.

6. Haider, M. I., Shah, T., Ali, A., Shah, D., & Khalid, I. (2022). Pseudo random sequences based on elliptic curve subgroups and mathematical model for its application to digital image security. *Multimedia Tools and Applications*, *81*(17), 23709-23734.

7. Shah, D., Shah, T., Khalid, I., & Riaz, N. (2022, August). Leveled Homomorphic Encryption Based on Finite Field Isomorphism Problem Over Matrix Algebra. In *2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 641-645). IEEE.

8. Gabr, M., Younis, H., Ibrahim, M., Alajmy, S., Khalid, I., Azab, E., ... & Alexan, W. (2022). Application of dna coding, the lorenz differential equations and a variation of the logistic map in a multi-stage cryptosystem. *Symmetry*, *14*(12), 2559.

Table of Contents

List of Figures

List of Tables

Chapter 1

Elliptic Curve and Cryptography: An Overview

1.1 Introduction

This chapter aims to summarize the fundamental theory just enough for cryptographic applications. Additionally, this chapter seeks the basic notation, concepts, and properties of an elliptic curve and cryptography, which are utilized in the imminent chapters. There are four primary divisions within the chapter. The elliptic curve's fundamental definitions and mathematical core functioning are covered in the second section. Next, Section three looks at the underlying mathematical operation of the Hyper elliptic curve (HEC). The third section of the chapter covers elliptic curve cryptography (ECC) and its cryptosystem. The study of algorithms and asymptotic complexity studies of the algorithms are enclosed in the last part of the chapter.

1.2 Fundamentals of Elliptic Curve

Throughout this subsection, $\mathbb{K}$ denotes a field of arbitrary characteristics, and $\mathbb{L}$ is the algebraic extension field of $\mathbb{K}$. The general reference of this section is given in Chapter 3 by Darrel Hankerson, Alfred Menezes, and Scott Vanstone [1], Chapter 1 of Lawrence Washington [2], and Chapter 13 by Dale Husemöller [3].

Definition 1.1. Let $a_0, a_1, \acute{a}_0, \acute{a}_1, \acute{a}_2 \in \mathbb{K}$. An elliptic curve over the field $\mathbb{K}$ is defined by the equation

$$\mathbb{E} = y^2 + a_0xy + a_1y = x^3 + \acute{a}_0x^2 + \acute{a}_1x + \acute{a}_2 \tag{1.1}$$

With discernment $\triangle_{\mathbb{E}} \neq 0$, the $\triangle_{\mathbb{E}}$, is defined as follows:

$$\begin{gathered}\triangle_{\mathbb{E}} = -\mathcal{D}_1{}^2\mathcal{D}_2 - 8\mathcal{D}_3{}^3 - 27\mathcal{D}_4{}^2 + 9\mathcal{D}_1\mathcal{D}_3\mathcal{D}_4 \\ \mathcal{D}_1 = a_0{}^2 + 4a_0 \\ \mathcal{D}_2 = a_0{}^2\acute{a}_2 + 4\acute{a}_0\acute{a}_2 - a_0a_1\acute{a}_1 + \acute{a}_0a_1{}^2 - \acute{a}_1{}^2 \\ \mathcal{D}_3 = 2\acute{a}_1 + a_0a_1 \\ \mathcal{D}_4 = a_1{}^3 + 4\acute{a}_2\end{gathered} \tag{1.2}$$

Then the set of $\mathbb{L}$-rational points on $\mathbb{E}$ along with the point of infinity is defined as:

$$\mathbb{E}\,(\mathbb{L}) = \{(x, y) \in \mathbb{L} \times \mathbb{L}: y^2 + a_0xy + a_1y - x^3 - \acute{a}_0x^2 - \acute{a}_1x - \acute{a}_2 = 0\} \cup \{\infty\} \tag{1.3}$$

Remarks 1.2. (Observation on Definition 1.1)

I. The above equation (1.3) is called the Weierstrass equation.

II. Because the coefficients $a_0, a_1, \acute{a}_0, \acute{a}_1, \acute{a}_2$ of its defining equation are elements of $\mathbb{K}$, we state that of $\mathbb{E}$ is defined over $\mathbb{K}$. When we write $\mathbb{E}/_{\mathbb{K}}$, we highlight that $\mathbb{E}$ is defined over $\mathbb{K}$ and $\mathbb{K}$ is referred to as the underlying field. Remember that if the elliptic curve $\mathbb{E}$ is defined over $\mathbb{K}$, it also be defined over any extension field of $\mathbb{K}$.

III. The condition of discriminant $\triangle_{\mathbb{E}} \neq 0$, guarantee that the $\mathbb{E}$ is "smooth," that is, there is not any point (x, y) where the curve has more than one unique tangent lines

IV. The infinity point (∞, ∞), generally denoted by ∞ sitting at the top of the y-axis as well as the bottom of the y-axis, satisfies the equation (1.3)

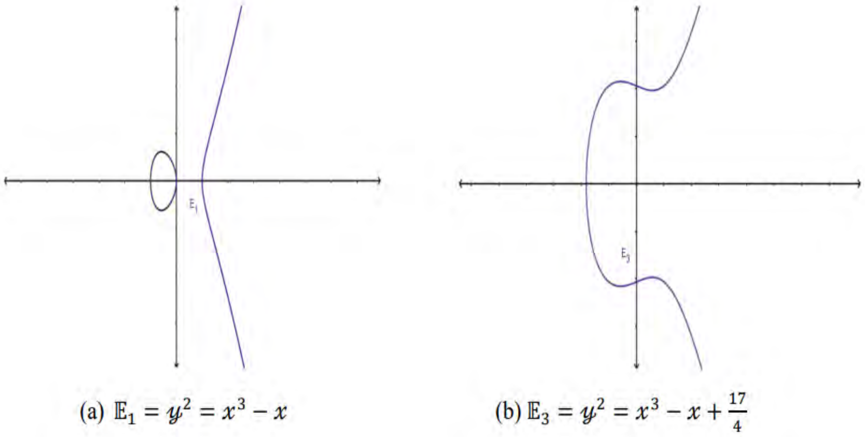
Example 1.3. (Elliptic curve over the field $\mathbb{K} = \mathbb{R}$). Let the elliptic curves

$$\mathbb{E}_1 = y^2 = x^3 - x \tag{1.4}$$

$$\mathbb{E}_2 = y^2 = x^3 + \frac{17}{8} \tag{1.5}$$

$$\mathbb{E}_3 = y^2 = x^3 - x + \frac{17}{4} \tag{1.6}$$

defined over the $\mathbb{K} = \mathbb{R}$. The graphical representations of equations (1.4) and (1.6) are illustrated in Figure 1.



(a) $\mathbb{E}_1 = y^2 = x^3 - x$

(b) $\mathbb{E}_3 = y^2 = x^3 - x + \frac{17}{4}$

Figure 1. Elliptic curve over R

1.2.1 Simplified Weierstrass equations

Definition 1.4. Consider the elliptic curves $\mathbb{E}$ and $\overline{\mathbb{E}}$ defined over the field $\mathbb{K}$ and given by the Weierstrass equation

$$\mathbb{E} = y^2 + a_0 xy + a_1 y = x^3 + \acute{a}_0 x^2 + \acute{a}_1 x + \acute{a}_2 \tag{1.7}$$

$$\overline{\mathbb{E}} = y^2 + \overline{a_0}xy + \overline{a_1}y = x^3 + \overline{\acute{a}_0}x^2 + \overline{\acute{a}_1}x + \overline{\acute{a}_2} \tag{1.8}$$

are said to be isomorphic over the field $\mathbb{K}$ if $\exists\ u, r, s, t\ \in \mathbb{K}$ with $u \neq 0$, in such a manner that the change of variables transforms equation (1.7) into equation (1.8).

$$(x, y) = \begin{cases} x \to u^2x + r \\ y \to u^3y + u^2sx + t \end{cases} \tag{1.9}$$

The change of variables defined in equation (1.9) is called admissible change of variables.

A general Weierstrass equation

$$\mathbb{E} = y^2 + a_0xy + a_1y = x^3 + \acute{a}_0x^2 + \acute{a}_1x + \acute{a}_2$$

Applying admissible change of variables can substantially simplify a Weierstrass equation. Throughout the rest of the thesis, simplified equations will be employed. In the case of underlying fields with different characteristic from 2 and 3, or underlying fields with characteristics equal to 2 or 3, we consider these cases separately.

Case 1. When the characteristics of the field $\mathbb{K} \neq 2,3$

If the characteristic of the field $\mathbb{K} \neq 2,3$, then the admissible change of the variable is defined as follows:

$$(x, y) \to \left(\frac{x - 3{a_0}^2 - 12\acute{a}_0}{36}, \frac{y - 3a_0x}{216} - \frac{{a_0}^3 + 4a_0\acute{a}_0 - 12a_1}{24}\right). \tag{1.10}$$

The above Transformation of the Weierstrass equation (1.7) into (1.11) is called the short Weierstrass equation

$$y^2 = x^3 + \mathrm{A}x + \mathrm{B}. \tag{1.11}$$

Where the elements $\mathrm{A}, \mathrm{B} \in \mathbb{K}$. The discriminant of the equation (1.11) is $\triangle_{\mathbb{E}} = -16(4\mathrm{A}^3 + 27\mathrm{B}^2)$.

Case 2. When the characteristics of the field $\mathbb{K} = 2$

There are two different sub-cases when the characteristic of the field is 2. In the first sub-case, if the coefficient $a_0 \neq 0$, then an admissible change of variable is:

$$(x, y) \to \left({a_0}^2x + \frac{a_1}{a_0}, {a_0}^3y + \frac{{a_0}^2\acute{a}_1 - {a_1}^2}{{a_0}^3}\right). \tag{1.12}$$

transforms $\mathbb{E}$ to the curve

$$y^2 + xy = x^3 + \mathrm{A}x^2 + \mathrm{B}, \tag{1.13}$$

where A, B are the elements of $\mathbb{K}$ and the discriminant $\triangle_{\mathbb{E}} = \mathrm{B}$. A curve of this type is called a non-supersingular which is discussed after this sub-section.

In the second sub-case, if the coefficient $a_0 = 0$, then the admissible change of variable

$$(x, y) \to (x + \acute{a}_0, y). \tag{1.14}$$

and transforms the curve to

$$y^2 + \mathbb{C}y = x^3 + \mathrm{A}x + \mathrm{B}, \tag{1.15}$$

where the coefficients $\mathbb{C}, \mathrm{A}, \mathrm{B}$ are in $\mathbb{K}$ and the discriminant $\triangle_{\mathbb{E}} = \mathbb{C}^4$. The curve defined above is known as supersingular.

Case 3. When the characteristics of the field $\mathbb{K} = 3$

There are also two different sub-cases when the characteristic of $\mathbb{K}$ is 3. In the first sub-case, if the coefficient ${a_0}^2 \neq -\acute{a}_0$ then an admissible change of variable is defined as follows:

$$(x, y) \to \left(x + \frac{\mathcal{D}_3}{\mathcal{D}_1}, y + a_0 x + a_0 \frac{\mathcal{D}_3}{\mathcal{D}_1} + a_1\right), \tag{1.16}$$

where $\mathcal{D}_3 = \acute{a}_1 - a_0 a_1$ and $\mathcal{D}_1 = {a_0}^2 + \acute{a}_0$. And transform into the curve

$$y^2 = x^3 + \mathrm{A}x + \mathrm{B}\,, \tag{1.17}$$

where the coefficients $\mathrm{A}, \mathrm{B} \in \mathbb{K}$ and his discriminant $\triangle_{\mathbb{E}} = -(\mathrm{A}^3\mathrm{B})$. In the second sub-case, if the coefficient ${a_0}^2 = -\acute{a}_0$ then the admissible change of variable is defined as follows :

$$(x, y) \to (x, y + a_0 x + a_1), \tag{1.18}$$

and transforms to the curve

$$y^2 = x^3 + \mathrm{A}x + \mathrm{B}, \tag{1.19}$$

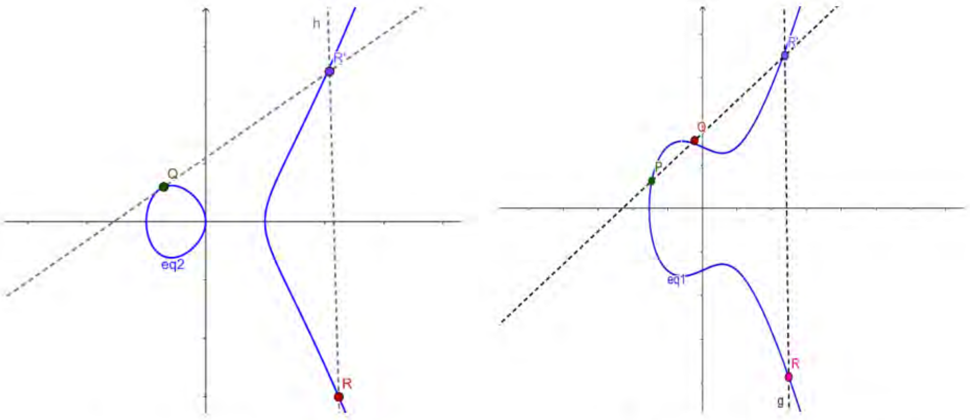
where the elements $\mathrm{A}, \mathrm{B} \in \mathbb{K}$ and the discriminant $\triangle_{\mathbb{E}} = -\mathrm{A}^3$. The curve defined in equations (1.17) and (1.19) is considered non-supersingular and supersingular, respectively.

1.2.2 Group law

To form a group law on the elliptic curve over the specified field $\mathbb{K}$, i.e., $\mathbb{E}(\mathbb{K})$. We start with any two points on the particular elliptic curve $\mathbb{E}(\mathbb{K})$. For adding two points in $\mathbb{E}(\mathbb{K})$ to get the third point in $\mathbb{E}$, use the chord-and-tangent rule. The collection of points $\mathbb{E}(\mathbb{K})$ with the binary operation of the addition define an abelian group with ∞ functioning as its identity. To avoid confusion of adding simply the coordinates of points, we denote the operation of the addition of points by $+_{\mathbb{E}}$.

Let $p = (x_1, y_1)$ and $\mathcal{Q} = (x_2, y_2)$ be two points on $\mathbb{E}(\mathbb{K})$. Then the addition of p and $\mathcal{Q}$, equal to $\mathcal{R}$, is defined as follows. First, draw the line $\mathcal{L}$ through the points p and $\mathcal{Q}$. From figure 2, we can see that the line $\mathcal{L}$ intersects $\mathbb{E}$ on the new point $\acute{\mathcal{R}}$. Reflect the point $\acute{\mathcal{R}}$ along the x-axis with a change in the sign of y coordinate to get the point $\mathcal{R}$. The Doubling of the point $\mathcal{Q}$ is defined as follows. First, draw the line $\mathcal{L}$ on the elliptic curve at the point $\mathcal{Q}$; the line $\mathcal{L}$ meet another point $\acute{\mathcal{R}}$ on the elliptic curve, $\mathbb{E}$. Reflect the point $\acute{\mathcal{R}}$ along the x-axis, we get the point $\mathcal{R}$ which is a doubling of the point $\mathcal{Q}$. The geometrical interpretation is shown in Figure 2.

The mathematical formulation of group law for simplified Weierstrass equations over different underlying fields for the supersingular and non-supersingular elliptic curve is presented in the following subsection.



(a) **Doubling**: $\mathcal{Q} +_{\mathbb{E}} \mathcal{Q} = \mathcal{R}$

(b) **Addition**: $p +_{\mathbb{E}} \mathcal{Q} = \mathcal{R}$

Figure 2. Geometric interpretation of point addition and doubling

1.2.3 Group law for $\mathbb{E}(\mathbb{K})$: $y^2 = x^3 + \mathrm{A}x + \mathrm{B}$, char($\mathbb{K}$) $\neq 2, 3$

I. Identity: $p +_{\mathbb{E}} \infty = \infty +_{\mathbb{E}} p = \infty$, $\forall\, p \in \mathbb{E}(\mathbb{K})$.

II. Inverse: If $p = (x_1, y_1) \in \mathbb{E}(\mathbb{K})$, then $(x_1, y_1) +_{\mathbb{E}} (x_1, -y_1) = \infty$. Where $(x_1, -y_1)$ is the inverse point of p denoted by $-p$. Moreover, the opposite $-p$ is in $\mathbb{E}(\mathbb{K})$

III. Addition of distinct point: Let $p = (x_1, y_1), \mathcal{Q} = (x_2, y_2) \in \mathbb{E}(\mathbb{K})$, where $p \neq \mp \mathcal{Q}$. Then $p + \mathcal{Q}$ computed using the following mathematical expressions.

$$\mathcal{R} = \wp +_{\mathbb{E}} \mathcal{Q} = (x_3, y_3),$$

where

$$x_3 = \mathfrak{m}^2 - x_1 - x_2 \text{ and } y_3 = \mathfrak{m}(x_1 - x_3) - y_1$$

and $\mathfrak{m}$ denotes the slope of line through the points of $\wp$ and $\mathcal{Q}$ which is :

$$\mathfrak{m} = \frac{y_2 - y_1}{x_2 - x_1}.$$

IV. Doubling: Let $\wp \in \mathbb{E}(\mathbb{K})$ where $\wp \neq -\wp$, then doubling of the point $\wp$ is denoted by $2\wp$ and computed by the following mathematical expression.

$$2\wp = \wp +_{\mathbb{E}} \wp = (\acute{x}_3, \acute{y}_3)$$

where

$$\acute{x}_3 = \mathfrak{m}^2 - 2x_1 \text{ and } \acute{y}_3 = \mathfrak{m}(x_1 - x_3) - y_1$$

and the slop $\mathfrak{m}$ of the line tangent to the curve in the point $\wp$ is:

$$\mathfrak{m} = \frac{3x^2 + \mathrm{A}}{2y}.$$

Example 1.5. (Elliptic Curve over the prime field). Consider the elliptic curve $\mathbb{E}$ over the prime field $\mathcal{F}_P$, with the parameters $\mathrm{A} = 1, \mathrm{B} = 11$ and $P = 41$

$$y^2 = x^3 + 1x + 11 \tag{1.20}$$

The $\triangle_{\mathbb{E}} = -16(4\mathrm{A}^3 + 27\mathrm{B}^2) = -16(4(1)^3 + 27(11)^2) = -52{,}336 \not\equiv 0 \bmod 41$, which shows that the curve is smooth. The points on $\mathbb{E}(\mathcal{F}_{41})$ are given below:

Table 1. No. of Points on $\mathbb{E}(\mathcal{F}_{41})$

∞	(8,11)	(16,33)	(20,35)	(36,2)
(21,2)	(8,30)	(17,12)	(22,12)	(36,39)
(2,29)	(10,18)	(17,29)	(22,29)	(37,5)
(3,0)	(10,23)	(18,11)	(24,1)	(37,36)
(5,10)	(11,0)	(18,30)	(24,40)	(39,1)
(5,31)	(15,11)	(19,1)	(25,9)	(39,40)
(7,19)	(15,30)	(19,40)	(25,32)	(40,3)
(7,22)	(16,8)	(20,6)	(27,0)	(40,38)

1.2.4 Group law for Non-Supersinguler $\mathbb{E}/_{\mathcal{F}_{2^m}}$: $y^2 + xy = x^3 + \mathrm{A}x^2 + \mathrm{B}$.

I. Identity: $\wp +_{\mathbb{E}} \infty = \infty +_{\mathbb{E}} \wp = \infty, \forall\, \wp \in \mathcal{F}_{2^m}$.

II. Inverse: If $\wp = (x_1, y_1) \in \mathcal{F}_{2^m}$, then $(x_1, y_1) +_{\mathbb{E}} (x_1, x_1 + y_1) = \infty$. Where $(x_1, x_1 + y_1)$, is the inverse point of $\wp$ denoted by $-\wp$. Moreover, the opposite point $-\wp \in \mathbb{E}(\mathbb{K})$.

III. Addition of distinct points**:** Let $\mathcal{p} = (x_1, y_1), \mathcal{Q} = (x_2, y_2) \in \mathcal{F}_{2^m}$, Where $\mathcal{p} \neq \mp \mathcal{Q}$. The addition of $\mathcal{p}$ and $\mathcal{Q}$ is defined as follows:

$$\mathcal{R} = \mathcal{p} +_{\mathbb{E}} \mathcal{Q} = (x_3, y_3),$$

where

$$x_3 = \mathfrak{m}^2 + \mathfrak{m} + x_1 + x_2 + \text{A} \text{ and } y_3 = \mathfrak{m}(x_1 + x_3) + x_3 + y_1$$

and $\mathfrak{m}$ as denoted is the slope of the points of $\mathcal{p}$ and $\mathcal{Q}$ defined as:

$$\mathfrak{m} = \frac{y_2 + y_1}{x_2 + x_1}.$$

IV. Doubling: Let $\mathcal{p} \in \mathcal{F}_{2^m}$. Where $\mathcal{p} \neq -\mathcal{p}$, doubling of the point $\mathcal{p}$ is denoted by $2\mathcal{p}$ and computed by the following mathematical expression.

$$2\mathcal{p} = \mathcal{p} +_{\mathbb{E}} \mathcal{p} = (\acute{x}_3, \acute{y}_3),$$

where

$$\acute{x}_3 = \mathfrak{m}^2 + \mathfrak{m} + \text{A} \text{ and } y_3 = (\mathfrak{m} + 1)\acute{x}_3 + {x_1}^2$$

and the slop of the point $\mathcal{p} = (x_1, y_1) \in \mathcal{F}_{2^m}$, is defined as follows:

$$\mathfrak{m} = {(y_1 + x_1)}/{x_1}$$

Example 1.6. (Non-Supersingular Elliptic Curve over $\mathbb{E}/_{\mathcal{F}_{2^5}}$). Consider the finite field $\mathcal{F}_{2^5}$ and $p(\mathcal{X}) = \mathcal{X}^5 + \mathcal{X}^2 + 1$ is the reduction of the polynomial in $\boldsymbol{\mathcal{F}_{2^5}}$**.** If τ is a root of $p(\mathcal{X})$, we have $p(\tau) = 0$, which implies that

$$p(\tau) = \tau^5 + \tau^2 + 1 = 0$$

$$\tau^5 = \tau^2 + 1 \tag{1.21}$$

Each of the 31 nonzero elements of $\boldsymbol{\mathcal{F}_{2^5}}$ will now be interpreted using equation (1.21) as shown in Table 2. Take note that we need just five coordinates to define each of the $P = 2^5$ components of $\mathcal{F}_{2^5}$.

Consider the non-supersingular elliptic curve with parameters $\text{A} = \tau^{11}$ and $\text{B} = \tau^{10}$ defined as follows:

$$y^2 + xy = x^3 + \tau^{11}x^2 + \tau^{10} \tag{1.22}$$

The number of rational points of the curve of equation (1.22) is shown in Table 3 below.

Table 2. Elements of $\mathcal{F}_{2^5}$

S.no	$Element\ in\ GF(2^m)$	$Polynomial$	$Coordinates$
0	0	0	00000
1	τ	τ	00010
2	τ^2	τ^2	00100
3	τ^3	τ^3	01000
4	τ^4	τ^4	10000
5	τ^5	$\tau^2 + 1$	00101
6	τ^6	$\tau^3 + \tau$	01010
7	τ^7	$\tau^4 + \tau^2$	10100
8	τ^8	$\tau^2 + 1 + \tau^3$	01101
9	τ^9	$\tau^4 + \tau + \tau^3$	11010
10	τ^{10}	$\tau^4 + 1$	10001
11	τ^{11}	$\tau^2 + \tau + 1$	00111
12	τ^{12}	$\tau^3 + \tau^2 + \tau$	01110
13	τ^{13}	$\tau^4 + \tau^2 + \tau^3$	11100
14	τ^{14}	$\tau^4 + \tau^2 + \tau^3 + 1$	11101
15	τ^{15}	$\tau^4 + \tau^2 + \tau + \tau^3 + 1$	11111
16	τ^{16}	$\tau^4 + \tau + \tau^3 + 1$	11011
17	τ^{17}	$\tau^4 + \tau + 1$	10011
18	τ^{18}	$\tau + 1$	00011
19	τ^{19}	$\tau^2 + \tau$	00110
20	τ^{20}	$\tau^3 + \tau^2$	01100
21	τ^{21}	$\tau^4 + \tau^3$	11000
22	τ^{22}	$\tau^4 + \tau^2 + 1$	10101
23	τ^{23}	$\tau^3 + \tau^2 + \tau + 1$	01111
24	τ^{24}	$\tau^4 + \tau^3 + \tau^2 + \tau$	11110
25	τ^{25}	$\tau^4 + \tau^3 + 1$	11001
26	τ^{26}	$\tau^4 + \tau^2 + \tau + 1$	10111
27	τ^{27}	$\tau^3 + \tau + 1$	01011
28	τ^{28}	$\tau^4 + \tau^2 + \tau$	10110
29	τ^{29}	$\tau^3 + 1$	01001
30	τ^{30}	$\tau^4 + \tau$	10010
31	τ^{31}	1	00001

Table 3. Number of valid points on $\mathcal{F}_{2^5}$

∞	(01011, 11110)	(11001, 01101)
(00000, 00101)	(01100, 00111)	(11001, 10100)
(00100, 11010)	(01100,01011)	(11010, 01100)
(00100, 11110)	(01111, 10011)	(11010, 10110)
(00110,10001)	(01111, 11100)	(11011, 01000)
(00110 ,10111)	(10010, 01001)	(11011,10011)
(00111, 01001)	(10010, 11011)	(11100,00110)
(00111, 01110)	(10011, 00000)	(11100, 11010)
(01000, 10110)	(10011, 10011)	(11101, 00010)
(01000, 11110)	(10101, 00011)	(11101, 11111)
(01010, 00100)	(10101, 10110)	(11111, 00101)
(01010, 01110)	(11000, 00101)	(11111,11010)
(01011, 10101	(11000, 11101)	

1.2.5 Group law for supersingular $^{\mathbb{E}}/_{\mathcal{F}_{2^m}}$: $y^2 + \mathbb{C}y = x^3 + \mathrm{A}x + \mathrm{B}$.

I. Identity: $p +_{\mathbb{E}} \infty = \infty +_{\mathbb{E}} p = \infty\,, \forall\, p \in \mathcal{F}_{2^m}$.

II. Inverse: If $p = (x_1, y_1) \in \mathcal{F}_{2^m}$, then $(x_1, y_1) +_{\mathbb{E}} (x_1, y_1 + \mathbb{C}) = \infty$. Where$(x_1, y_1 + \mathbb{C})$ is the opposite $-p$ of p denoted by. Moreover, the opposite $-p$ is in $\mathbb{E}(\mathbb{K})$.

III. Addition of distinct Points: Let $p = (x_1, y_1) \in \mathcal{F}_{2^m}$ and $\mathcal{Q} = (x_2, y_2) \in \mathcal{F}_{2^m}$ Where $p \neq \mp \mathcal{Q}$. Then the sum of p and $\mathcal{Q}$ is:

$$\mathcal{R} = p +_{\mathbb{E}} \mathcal{Q} = (x_3, y_3),$$

where

$$x_3 = \mathfrak{m}^2 + x_1 + x_2$$
$$y_3 = \mathbb{C} + y_1 + \mathfrak{m}(x_1 + x_3)$$

and $\mathfrak{m}$ is denoted as the slope of the points of p and $\mathcal{Q}$ defined as:

$$\mathfrak{m} = \frac{y_2 + y_1}{x_2 + x_1}.$$

IV. Point doubling: Let $p = (x_1, y_1) \in \mathcal{F}_{2^m}$. Where $p \neq -p$, doubling of the point p is denoted by $2p$ and computed by the following mathematical expression:

$$2p = p +_{\mathbb{E}} p = (\acute{x}_3, \acute{y}_3),$$

where $\acute{x}_3 = \frac{({x_1}^2 + \mathrm{A})^2}{\mathbb{C}}$ and $\acute{y}_3 = \left(\frac{({x_1}^2 + \mathrm{A})}{\mathbb{C}}\right)(x_1 + \acute{x}_3) + y_1 + \mathbb{C}$.

1.2.6 Scalar multiplication of point

Using the previously established operation, let $\mathbb{G}$ represent the abelian group formed by the points on the elliptic curve $\mathbb{E}(\mathcal{F}_P)$. By continually adding the point P multiple time equal to the scalar's value, we may define the multiplication by scalar T on $\mathbb{E}(\mathcal{F}_P)$.

$$TP = \underbrace{P +_{\mathbb{E}} P +_{\mathbb{E}} P +_{\mathbb{E}} P +_{\mathbb{E}} \ldots, \ldots +_{\mathbb{E}} P}_{T} \qquad (1.23)$$

1.2.7 Order and Structure of the Group

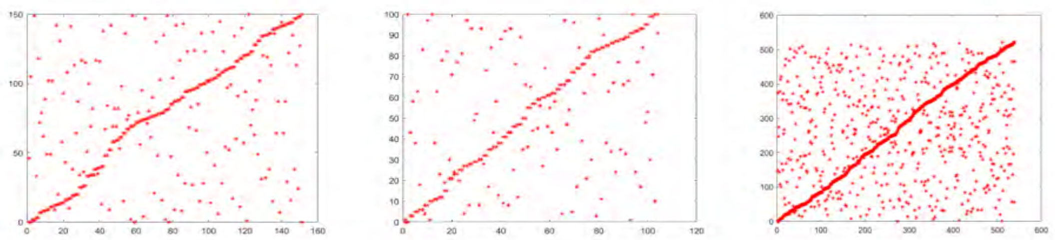
Let the elliptic curve $\mathbb{E}$ over the field $\mathcal{F}_P$. The order of $\mathbb{E}(\mathcal{F}_P)$ represented by $\#\mathbb{E}(\mathcal{F}_P)$, which shows the number of points on the given elliptic curve $\mathbb{E}(\mathcal{F}_P)$. Moreover, $\#\mathbb{E}(\mathcal{F}_P) \in [1, 2P + 1]$ because for each value of the x-coordinate, there are precisely two solutions in $\mathcal{F}_P$, of the Weierstrass equation (1.1). Tighter bounds on $\#\mathbb{E}(\mathcal{F}_P)$ are provided by the following Hasse's theorem.

Theorem 1.7. *Let the elliptic curve $\mathbb{E}$ over the field $\mathcal{F}_P$. Then*

$$P + 1 - 2\sqrt{P} \leq \#\mathbb{E}(\mathcal{F}_P) \leq P + 1 + 2\sqrt{P}$$

The interval $[P + 1 - 2\sqrt{P}, P + 1 + 2\sqrt{P}]$ is called the Hasse interval.

What types of groups can exist as group $\mathbb{E}(\mathcal{F}_P)$ is a natural question. The following two theorems answer to this question.



$(\boldsymbol{a})\#(\mathbb{E}_1^2(\mathcal{F}_{151})) = 152$ $(\boldsymbol{b})\#(\mathbb{E}_1^1(\mathcal{F}_{101})) = 105$ $(\boldsymbol{c})\#(\mathbb{E}_{11}^{22}(\mathcal{F}_{521})) = 540$

Figure 3. Number of points on elliptic curve module P

Theorem 1.8. *Let $\acute{P} = P^m$, where P is the characteristics of $\mathcal{F}_{\acute{P}}$. And let $\mathcal{N} = \acute{P} + 1 - t$. Then there is $\mathbb{E}(\mathcal{F}_{\acute{P}})$ such that $\mathcal{N} = \#\mathbb{E}(\mathcal{F}_{\acute{P}})$ if and only if $2\sqrt{\acute{P}} \geq |t|$ and the following conditions hold.*

i. $gcd(a, P) = 1$.

ii. *If m is even and $t = \pm 2\sqrt{\acute{P}}$.*

iii. *If m is even, $P \not\equiv 1 mod\ 3$ and $t = \pm\sqrt{\acute{P}}$.*

iv. *If m is odd, $P = 3$ or 2 and $t = \pm P^{{m+1}/{2}}$.*

v. *If m is even, $P \not\equiv 1 mod\ 4$ and $t = 0$.*

vi. *If m is odd and $t = 0$.*

Theorem 1.9. *Let $\mathcal{N}$ be the order of the elliptic curve over a finite field $\mathcal{F}_P$. Write $\mathcal{N} = P^c\mathcal{N}_1\mathcal{N}_2$ with $\mathcal{N}_1/\mathcal{N}_2$ and $P \nmid \mathcal{N}_1\mathcal{N}_2$. Then there is an elliptic curve $\mathbb{E}(\mathcal{F}_P)$ such that* $\mathbb{E}(\mathcal{F}_P) = \mathbb{Z}_{\mathcal{N}_1} \oplus \mathbb{Z}_{\mathcal{N}_2} \oplus \mathbb{Z}_{P^c}$.

If and only if

i. $\mathcal{N}_1 = \mathcal{N}_2$ *for the case of (ii) with Theorem 1.8.*

ii. $\mathcal{N}_1/\acute{P} - 1$ *for the cases of (i, iii, iv, vi) with theorem 1.8.*

Example 1.10. (Order of elliptic curve over the field $(\mathcal{F}_{41})$). Consider the elliptic curve $\mathbb{E}$ over the prime field with $P = 41$ and $\mathrm{A}, \mathrm{B} \in \mathcal{F}_{41}$ of equation:

$$y^2 = x^3 + \mathrm{A}x + \mathrm{B}\ mod\ 41.$$

From the list of Table 4 shows every pair of coefficients (A,B) from the field $\mathcal{F}_{41}$ there exist integers $\mathcal{N}$ in the Hasse interval $\left[41+1-2\sqrt{41}, 41+1+2\sqrt{41}\right] = [29.19376, 54.80624]$.

Table 4. Admissible order of elliptic curve over $\mathbb{E}(\mathcal{F}_{41})$

$\mathcal{N}$	$(\mathbf{A},\mathbf{B})$	$\mathcal{N}$	$(\mathbf{A},\mathbf{B})$	$\mathcal{N}$	$(\mathbf{A},\mathbf{B})$	$\mathcal{N}$	$(\mathbf{A},\mathbf{B})$	$\mathcal{N}$	$(\mathbf{A},\mathbf{B})$
39	(1,3)	36	(10,30)	44	(23,34)	42	(35,38)	44	(19,4)
44	(2,5)	48	(31,33)	40	(5,8)	43	(11,33)	36	(10,30)
42	(0,3)	50	(17,21)	39	(6,17)	42	(13,32)	33	(11,32)
43	(7,4)	42	(0,18)	34	(12,14)	40	(24,34)	33	(12,2)
36	(9,6)	32	(25,0)	48	(8,31)	50	(28,29)	33	(13,4)
48	(11,13)	42	(24,36)	48	(9,23)	52	(20,30)	40	(4,35)
49	(21,35)	51	(16,20)	39	(27,7)	49	(39,19)	48	(7,27)
42	(0,8)	43	(15,28)	36	(19,1)	42	(14,1)	44	(8,40)
51	(1,8)	34	(13,28)	40	(24,7)	46	(39,17)	41	(11,40)
41	(3,8)	40	(1,2)	52	(12,19)	51	(17,38)	48	(39,40)
40	(5,8)	47	(14,7)	40	(25,38)	40	(25,38)	42	(22,39)

Example 1.11. (Group Structure of elliptic curve over the field $(\mathcal{F}_{31})$). Let the elliptic curve with the parameters $P = 31$ and $\mathrm{A} = 1, \mathrm{B} = 3 \in \mathcal{F}_{31}$ given by the following mathematical expression.

$$y^2 = x^3 + 1x + 3\ mod\ 31$$

The number of points $\mathcal{N} = \#\mathbb{E}(\mathcal{F}_{31}) = 41$. Since the group order is prime, the given elliptic curve is a cyclic group and any point from the given elliptic curve except for ∞, generates all the points of $\mathbb{E}(\mathcal{F}_{31})$. For instance, suppose that the point $\wp = (6,15)$; the successive multiplication of the point $\wp$ yield all the points of the group, as shown in Table 5.

Table 5. Successive multiplication of the point $\wp = (6,15)$

$\wp = (6,15)$	$10\wp = (3,23)$	$19\wp = (23,14)$	$28\wp = (4,28)$	$37\wp = (12,10)$
$2\wp = (27,11)$	$11\wp = (5,3)$	$20\wp = (30,1)$	$29\wp = (9,20)$	$38\wp = (18,26)$
$3\wp = (18,5)$	$12\wp = (9,11)$	$21\wp = (30,30)$	$30\wp = (5,28)$	$39\wp = (27,20)$
$4\wp = (12,21)$	$13\wp = (4,3)$	$22\wp = (23,17)$	$31\wp = (3,8)$	$40\wp = (6,16)$
$5\wp = (14,8)$	$14\wp = (26,20)$	$23\wp = (21,27)$	$32\wp = (24,5)$	$41\wp = (\infty)$
$6\wp = (20,5)$	$15\wp = (1,25)$	$24\wp = (22,28)$	$33\wp = (17,29)$	
$7\wp = (15,18)$	$16\wp = (28,29)$	$25\wp = (28,2)$	$34\wp = (15,13)$	
$8\wp = (17,2)$	$17\wp = (22,2)$	$26\wp = (1,6)$	$35\wp = (20,26)$	
$9\wp = (24,26)$	$18\wp = (21,4)$	$27\wp = (26,11)$	$36\wp = (14,23)$	

1.3 Hyper Elliptic Curve

Theoretically, all established public key cryptosystems are less secure than Hyper Elliptic Curve Cryptography (HECC). This is because, even when compared to Elliptic Curve Cryptosystems with equivalent key lengths, there is a high amount of mathematical complexity.

The mathematical foundation of a hyperelliptic curve (HEC) is thoroughly addressed in this subsection, and effective group operation methods are investigated. The group law in the HEC cryptosystem involves addition and doubling in the jacobian of the curve. Cantor provided the algorithm for the group operation. Further detail of this subsection can be found in Chapter 14 of H.Cohen and G.Frey [4], Chapter 21 of Stein and Alf [5] and from the research article [6]–[10].

Definition 1.12. (Hyper Elliptic Curve). A hyperelliptic curve $\mathcal{C}$ over the field $\mathbb{K}$ of genus $\mathcal{G} > 1$ is defined by the following equation.

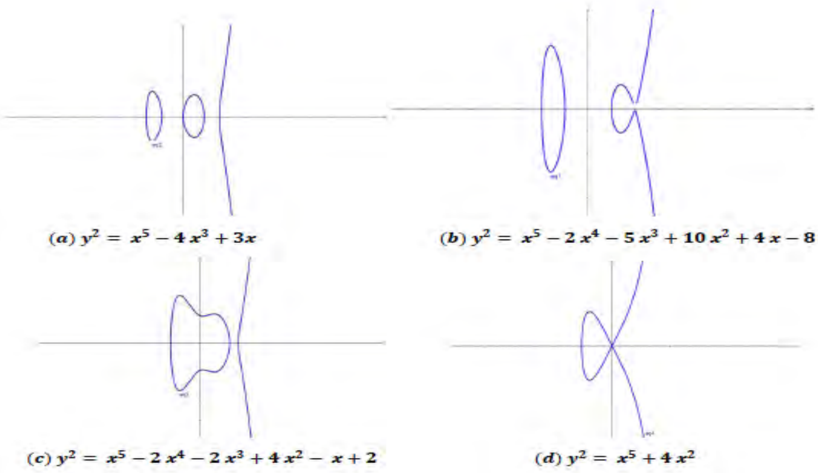
$$\mathcal{C}: \mathcal{Y}^2 + H(x)\mathcal{Y} = \mathrm{F}(x). \tag{1.24}$$

Where $H(x), \mathrm{F}(x) \in \mathbb{K}[x]$ polynomial of degree $\mathcal{G}$ and $2\mathcal{G} + 1$, respectively. And there is no such point on the curve $\mathcal{C}$ over the algebraic field $\mathbb{L}$ of $\mathbb{K}$, which fulfills the following conditions defined in equations 1.25 and 1.26, respectively.

$$\frac{d\mathcal{C}}{dx} = \acute{H}\mathcal{Y} - \acute{\mathrm{F}} = 0, \tag{1.25}$$

$$\frac{d\mathcal{C}}{d\mathcal{Y}} = 2\mathcal{Y} + \acute{H}. \tag{1.26}$$

Definition 1.13. (Rational, finite points, point of infinity of hyperelliptic curve). A point $P = (x, y) \in \mathbb{L} \times \mathbb{L}$ is said to be the rational point of the hyperelliptic curve $\mathcal{C}$, which satisfies equation 1.24. The collection of all points with a point of infinity ∞ is called the set of $\mathbb{L}$ −rational points represented by $\mathcal{C}(\mathbb{L})$.



(a) $y^2 = x^5 - 4x^3 + 3x$

(b) $y^2 = x^5 - 2x^4 - 5x^3 + 10x^2 + 4x - 8$

(c) $y^2 = x^5 - 2x^4 - 2x^3 + 4x^2 - x + 2$

(d) $y^2 = x^5 + 4x^2$

Figure 4. Geometric interpretation of different HEC

1.3.1 Group Arithmetic Operation on Hyper Elliptic Curve

In elliptic curves, we may construct a group by connecting the points on the curve with the point of ∞. However, in HEC, the collections of points with the point of ∞ cannot form a group. To make a group concerning the points of a hyperelliptic curve, we must first take the sum of the points as group components and then execute point addition like $(\mathfrak{p}_1 + \mathfrak{p}_2) \oplus (\mathfrak{q}_1 + \mathfrak{q}_2) = (\mathfrak{r}_1 + \mathfrak{r}_2)$. The symbols $\oplus$ and + do not represent xor and addition operations, respectively. Figure 5 below depicts an HEC for a genus 2 over the finite field $\mathcal{F}_P$, defined by the equation $\mathcal{C}: \mathcal{Y}^2 + H(x)\mathcal{Y} = \mathrm{F}(x)$. Before performing a group operation on this curve equation, we must satisfy the following five conditions.

i. $H(x), \mathrm{F}(x) \in \mathcal{F}_P[x]$.

ii. $\mathrm{F}(x)$ must be a monic polynomial, and the degree of $\mathrm{F}(x)$ is $2\mathcal{G} + 1(odd)$.

iii. The curve $\mathcal{C}(\mathcal{F}_P)$ does not have any singular point.

iv. $H(x) = 0$ if the field's characteristics are not equal to 2 and $\deg(H) \leq \mathcal{G}$, if the field's characteristics are equal to 2.

v. If the field's characteristics are equal to 2, then $\mathcal{Y}^2 = \mathrm{F}(x)$, is monic, odd degree and square free.

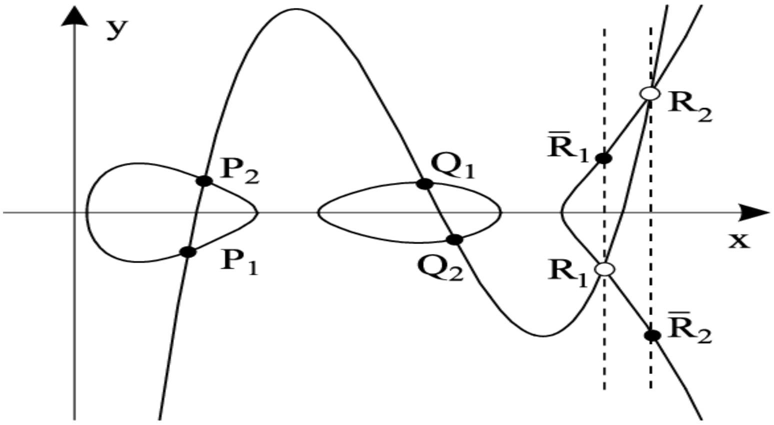


Figure 5. Group operation of HEC of genus 2.

As previously stated in section 1.2.2, the chord and tangent approach cannot be applied in the hyperelliptic curve. Unlike the chord and tangent approach in the elliptic curve, the Jacobian curve intersects at 5 points instead of just 3 in the elliptic curve. To construct a group, we use the quotient group which is the sum of the crossing points of the Jacobian variety curve with the hyperelliptic curve by the subset of the points that lie on the HEC.

1.4 Elliptic Curve Cryptography

Researchers spent much time investigating cryptographic systems based on more trustworthy trapdoor functions. However, in 1985 they successfully found a new approach, one based on elliptic curves, which was then proposed as the group's foundation for the discrete logarithm problem. Their application in cryptography relies mainly on the presence of a group law, which enables them for public key cryptography because their discrete logarithm problem is challenging as compared to the size of the parameters they employ. Therefore, elliptic curve cryptography (ECC) is a potent cryptography approach that may be used as an alternative to RSA. Using the core arithmetic of EC creates security between key pairs for public key encryption. ECC slowly gained popularity in recent years due to its smaller key size and ability to maintain security, as opposed to RSA, which uses prime numbers instead of elliptic curves. In light of the growing size of keys, this trend is likely to continue as devices increasingly depend on mobile resources to remain secure. Comparatively to RSA, ECC relies on the mathematical structure of EC over finite fields to construct public key cryptographic systems. Therefore, ECC generates keys that are mathematically harder to crack. In this respect, ECC has been deemed the leading-edge implementation of public key cryptography and is considered more secure than RSA. The adoption of ECC also ensures high levels of performance and security. It is because ECC is increasingly used as websites strive to enhance customer data security and mobile optimization at the same time. Furthermore, the applications of ECC, like the discrete logarithm problem of EC (ECDLP), the Diffie- hellman key exchange protocol based on EC, and the analogue of the EC-ElGamal public key cryptosystem are covered in this subsection.

The general references of this sub-section from chapter 5 of Hoffstein, Jeffrey, Jill Pipher, Joseph H. Silverman [11], Chapter 1 of Lawrence Washington [2], section 3 of Olga shevchuk [12] and [13]–[15].

1.4.1 Elliptic Curve Encryption Decryption

Since ECC is asymmetric key cryptography, the secret and public key pair generation must be required for communicating with two parties, Alice and Bob, over the insecure channel. Both parties initially agreed on standard EC over the finite field and generator $\mathbb{G}$ of large order. The generation of private and public keys is computed as follows. First, Alice and Bob choose their private key $\mathcal{A}_n$ and $\mathcal{B}_n$, respectively. The following mathematical expression executes the generation of the public key.

$$\mathcal{A}_p = \mathcal{A}_n\, \mathbb{G},\; \mathcal{B}_p = \mathcal{B}_n\, \mathbb{G}. \tag{1.27}$$

If Bob wants to send the message $\mathcal{P}_m$ to Alice. Bob encrypts the message $\mathcal{P}_m$, using the Alic public key pair. The mathematical expression of the encrypting procedure defined is followed:

$$\mathcal{C}_m = \{\mathcal{K}\mathbb{G},\; \mathcal{K}\mathcal{A}_p +_{\mathbb{E}} \mathcal{P}_m\}. \tag{1.28}$$

Where $\mathcal{K}$ is another random integer that ensures that even for the same plaintext point, the encrypted message generated by equation (1.28) differs each time, which makes it difficult for anyone trying to decipher the message correctly. Alice decrypts the message $\mathcal{P}_m$ by subtracting the coordinate of $\mathcal{K}\mathbb{G}$ multiplied by $\mathcal{A}_n$.

$$\mathcal{P}_m = \{\; \mathcal{P}_m +_{\mathbb{E}} \mathcal{K}\mathcal{A}_p - \mathcal{A}_n\mathcal{K}\mathbb{G}\}. \tag{1.29}$$

1.4.2 Elliptic Curve Discrete logarithm Problem (ECDLP)

Generally, to build the cryptosystem based on the discrete logarithm problem (DLP) over a finite field $\mathcal{F}^*{}_{\mathcal{P}}$. Alice publishes the numbers $\hbar$, the generator g and the exponent x to solve the following congruence relation

$$\hbar \equiv g^x.$$

Let us consider how Alice could accomplish a similar task using an elliptic curve $\mathbb{E}$ over $\mathcal{F}_P$. In a discrete logarithm problem, Alice's adversary Eve has to find an integer x such that g and $\hbar$ are elements of the group $\mathcal{F}^*{}_{\mathcal{P}}$.

$$\hbar \equiv \underbrace{\boldsymbol{g}.\boldsymbol{g}.\boldsymbol{g}, \dots, \dots, \boldsymbol{g}}_{x-\boldsymbol{time}\ multiplication}$$

Eve must figure out how many times g multiplied by itself to reach $\hbar$.

With the above mathematical formulation, which is based on the finite filed multiplicative group, Alice executed the same work with points of $\mathbb{E}(\mathcal{F}_P)$, for this, she picks the two points that say $\mathcal{R}_1$ and $\mathcal{R}_2$ in $\mathbb{E}(\mathcal{F}_P)$ and that private key of Alice T that makes

$$\mathcal{R}_1 = \underbrace{\mathcal{R}_2 +_{\mathbb{E}} \mathcal{R}_2 +_{\mathbb{E}} \mathcal{R}_2 +_{\mathbb{E}} \dots, \dots +_{\mathbb{E}} \mathcal{R}_2}_{T-times\ EC-\ addition} = T\mathcal{R}_2. \tag{1.31}$$

Then the eavesdropper, Eve, need to check out the sceat key T, by guessing how many time the point $\mathcal{R}_2$ must be added to itself to get the point $\mathcal{R}_1$.

Definition 1.14. (ECDLP). Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be the two points in $\mathbb{E}(\mathcal{F}_P)$. Then the ECDLP is the problem of finding an integer T such that $\mathcal{R}_1 = T\mathcal{R}_2$. By analogy with DLP based on finite field $\mathcal{F}^*{}_{\mathcal{P}}$, the representation of integer T is defined as.

$$T = \log_2 \mathcal{R}_1 \tag{1.32}$$

And the integer T is said to be the ECDLP of $\mathcal{R}_1$ with respect to $\mathcal{R}_2$.

1.4.3 The Elliptic Diffie–Hellman Key Exchange

In order to exchange data using a symmetric encryption technique like DES or AES, Alice and Bob need to come to terms with a shared key. For instance, Alice and Bob may be banks that need to send financial data. Using a courier to deliver the key is impracticable and time-consuming. Additionally, since Alice and Bob are presumed to have never met before, their sole means of communication are open channels. According to Diffie and Hellman, the following technique can create a shared secret key between the two communicating parties.

Procedure: Before the transmission of the data, Alice and Bob agree on the given $\mathbb{E}$ with parameters $\mathrm{A}, \mathrm{B} \in \mathcal{F}_P$, and the base point $\mathbb{G}$ of large prime order (usually the point $\mathbb{G}$ to be chosen of large prime order).

$$y^2 = x^3 + \mathrm{A}x + \mathrm{B}\, mod\ P$$

Alice and Bob choose the secret integers T_1 and T_2 and compute their public keys by the following mathematical expression.

$$\mathcal{A}_p = T_1\mathbb{G},\ \mathcal{B}_p = T_2\mathbb{G} \tag{1.33}$$

After that exchange their public keys $\mathcal{A}_p$ and $\mathcal{B}_p$ to execute the shared secret key between Alice and Bob, both the communicating parties multiply their secret keys to compute $T_2\mathcal{A}_p$ and $T_1\mathcal{B}_p$ respectively, which they may utilize as a key to secretly communicate using symmetric encryption.

$$T_2\mathcal{A}_p = T_2T_1(\mathbb{G}) = T_1\mathcal{B}_p \tag{1.34}$$

The key exchange for elliptic Diffie-Hellman is summarised in Table 6.

Example 1.15. Let the two communicating parties, Alice and Bob, decide to use ECDH key exchange protocol with the following parameters $A = 1, \mathrm{B} = 3, P = 31$ and point $\mathbb{G} = (15,13)$:

$$y^2 = x^3 + 1x + 3\, mod\ 31.$$

Alice and bob choose their private keys values $T_1 = 13$ and $T_2 = 17$ and then,

$$\text{Alice computes } \mathcal{A}_p = 13(15,13) = (24,5) \in \mathbb{E}(\mathcal{F}_{31}).$$

$$\text{Bob computes } \mathcal{B}_p = 17(15,13) = (12,21) \in \mathbb{E}(\mathcal{F}_{31}).$$

Both Alice and Bob send their public keys $\mathcal{A}_p$ and $\mathcal{B}_p$ over the insecure channel and, finally, computes the shared secret keys.

$$\text{Alice computes } T_1\mathcal{B}_p = 13(12,21) = (5,3) \in \mathbb{E}(\mathcal{F}_{31}).$$

$$\text{Bob computes } T_2\mathcal{A}_p = 17(24,5) = (5,3) \in \mathbb{E}(\mathcal{F}_{31}).$$

Eve can use the ECDLP to figure out Alice and Bob's secret. The only information that the eavesdropper Eve observes is the given EC, the finite field $\mathcal{F}_P$ and the points, $\mathcal{A}_p$ and $\mathcal{B}_p$. As a result, Eve must address the following problem.

Definition 1.16. (ECDHP). Let the elliptic curve $\mathbb{E}$ over a finite field $\mathcal{F}_P$ and consider the base point $\mathbb{G} \in \mathbb{E}(\mathcal{F}_P)$. The problem of calculating the value of $T_2T_1(\mathbb{G})$ from the known values of $T_1\mathbb{G}$ and $T_2\mathbb{G}$ is known as the Elliptic Curve Diffie-Hellman Problem (ECDHP).

Table 6. ECDH key exchange protocol

Public Parameters	
Large prime P, $\mathbb{E}: y^2 = x^3 + \mathrm{A}x + \mathrm{B}$, and the point $\mathbb{G}$(large prime order)	
Secret reckoning	
Alice • Chooses a secret integer T_1. • Computes the public point $\mathcal{A}_\mathrm{p} = \mathrm{T}_1\mathbb{G}$	**Bob** • Chooses a secret integer T_2. • Computes the public point $\mathcal{B}_\mathrm{p} = \mathrm{T}_2\mathbb{G}$
The Public exchange of values	
Alice sends $\mathcal{A}_\mathrm{p}$ To Bob: ⟶	$\boldsymbol{\mathcal{A}_\mathrm{p}}$
$\boldsymbol{\mathcal{B}_\mathrm{p}}$ ⟵	: Bob sends $\mathcal{B}_\mathrm{p}$ to Alice
More private reckoning	
Alice Computes the point $\mathrm{T}_1\mathcal{B}_\mathrm{p}$	**Bob** Computes the point $\mathrm{T}_2\mathcal{A}_\mathrm{p}$
Shared secret key	
The shared secret key between Alice and Bob is: $\mathrm{T}_2\mathcal{A}_\mathrm{p} = \mathrm{T}_2\mathrm{T}_1(\mathbb{G}) = \mathrm{T}_1\mathcal{B}_\mathrm{p}$	

1.4.4 The Elliptic ElGamal Public key Cryptosystem

Alice wants to communicate with Bob. The first thing Bob does is that he creates his public key. To make the discrete log problem difficult for elliptic curve $\mathbb{E}(\mathcal{F}_P)$, he selects the elliptic curve $\mathbb{E}$ over a finite field $\mathcal{F}_P$ and choose the base point $\mathbb{G} \in \mathbb{E}(\mathcal{F}_P)$. Bob also picks the secret integer T_2 and computes the public point $\mathcal{B}_p = T_2\mathbb{G}$ and publish the curve $\mathbb{E}$, the point $\mathbb{G}$ and the finite field $\mathcal{F}_P$, over the public channel. To send a message to Bob, Alice downloads the public parameter. The plaintext point $\mathcal{R} \in \mathbb{E}(\mathcal{F}_P)$**.** After that, Alice chooses the ephemeral key $\mathbb{K}$ and calculates the two cipher texts by the following mathematical expression.

$$\mathcal{C}_1 = \mathbb{K}\mathbb{G} \text{ and } \mathcal{C}_2 = \mathcal{R} + \mathbb{K}\,\mathcal{B}_p$$

Send the pair of cipher text $(\mathcal{C}_1, \mathcal{C}_1)$ to Bob, who computes

$$\mathcal{C}_2 - T_2\mathcal{C}_1 = \left(\mathcal{R} + \mathbb{K}\,\mathcal{B}_p\right) - T_2(\mathbb{K}\mathbb{G}) = \left(\mathcal{R} + \mathbb{K}(T_2\mathbb{G})\right) - T_2(\mathbb{K}\mathbb{G}) = \mathcal{R}.$$

1.5 Complexity Theory

Security is an important component of any cryptosystem since it determines how well the encryption method can resist attacks of different types. The complexity of the encryption algorithm is theoretically involved. It is generally based on some hard problem that is difficult to solve, and an encryption algorithm is devised. These problems relating to classical encryption were either number theoretic or combinatorial, whereas group-based cryptography might relate to group theory. For example, the discrete log problem is a legitimate cryptographic problem since it is hard to solve theoretically and practically. Cryptography uses a hard-to-solve problem to construct a trapdoor function whose inverse is connected to the solution. We would need the secret key for this trapdoor function to accomplish the challenging task. Complexity theory is an essential part of theoretical computer science that is relevant to quantifying the difficulty of a problem. In this section, we discuss some basic notations related to complexity theory.

Moreover, this section briefly discusses the basic definition of complexity theory. The intention of this section is not to describe the implementation guide of the algorithms. However, it sketches some crucial notions and results of complexity that are used later in this thesis. More detail of this subsection from chapter 3 of Baumslag, G., Fine, B., Kreuzer, M., & Rosenberger [16], chapter 1 of Mollin, R. A. [17], chapter 11 of Schneier, B. [18].

Definition 1.17. (Computational problem). A problem specified by a specific form of input and output is called a computational problem. The computational problem input and output instances are particular instances. The size of the computational problem input is the number of bits necessitated to symbolize the input.

Definition 1.18. (Computational Complexity). The algorithm's complexity is the maximum number of bit operations (addition, subtraction, division and multiplication of any two binary digits) necessities for the algorithm to solve the computational problem. The upper bound on the complexity is denoted by big oh 'O' notation. Whenever the complexity estimate of the algorithm is given in terms of O then we assume that there are infinite numbers of countable inputs to that algorithm. The computational complexity of an algorithm, or just complexity, is the total number of bit operations required to accomplish the algorithm's performance.

Definition 1.19 (Big oh O notation). Let f and g be two real-valued functions $f, g: \mathbb{N} \longrightarrow \mathbb{Z}^+$, then $f = O(g)$ if there exists $c \in \mathcal{R}_{>0}$ and a natural number $\mathcal{N}$, such that

$$f(m) \leq cg(m). \qquad \text{for all } m \geq \mathcal{N}$$

Similarly, if $f(m_1, m_2 \dots, m_k)$ and $g(m_1, m_2 \dots, m_k)$ be two functions from $\mathbb{N}^k$ to $\mathcal{R}_{>0}$, then $f = O(g)$ if there exists $c \in \mathcal{R}_{>0}$ and $N_1, N_2, \dots, N_k \in \mathbb{N}$ such that $f(m_1, m_2 \dots, m_k) \leq cg(m_1, m_2 \dots, m_k)$ with $m_i > N_i$. for all $1 \leq i \leq k$.

Theorem 1.20. (Properties of O). *Let f and g be two real-valued functions $f, g: \mathbb{N} \longrightarrow \mathbb{Z}^+$, then*

i. *If $c \in \mathcal{R}_{>0}$, then $cO(g) = O(g)$.*

ii. $O(fg) = O(f)O(g)$.

iii. $O(max\{fg\}) = O(f) + O(g)$.

Example 1.21. $12m^3 + 10n^2 + 17n + 122 = O(m^3)$, $\sin(m) + \cos(m) + m = O(m)$, $2^m + m^{10} = O(2^m)$ and $\log_n(m) = O(\log(m))$.

Definition 1.22. Let f and g be two real-valued functions $f, g: \mathbb{N} \longrightarrow \mathbb{Z}^+$, then $f = O(g)$ if

$$\underset{m\to\infty}{\text{limit}} \frac{f(m)}{g(m)} = 0.$$

The function may be expressed as; $f = \tilde{O}(g)$ if there exists $n \in \mathbb{N}$ such that $f(m) = O(g(m) \log(g(m))^n)$. The function $f = \Omega(g)$ if $g = O(f)$ and $f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$.

Definition 1.23. Assume that $\mathcal{A}$ is an algorithm and that $\mathcal{T}(m)$ is the maximum running time that $\mathcal{A}$ may take to solve any problem with the size of m bits.

i. An Algorithm $\mathcal{A}$ is said to be polynomial time(PT), if there exists a positive integer i such that $\mathcal{T}(m) = O(m^i)$.

ii. An Algorithm $\mathcal{A}$ is said to be super polynomial-time(SPT) if for all $c \in \mathcal{R}_{>1}$ the upper bound $\mathcal{T}(m) = \Omega(m^c)$.

iii. An Algorithm A is said to be exponential time(ET) if there exists a constant $c \in \mathcal{R}_{>1}$ such that $\mathcal{T}(m) = O(c^m)$.

The above definition is for uniform complexity, as all the problem instances are solved through a single algorithm $\mathcal{A}$. In non-uniform complexity, for each positive integer m and input $\hbar(m)$ of polynomial-size, if x is a string of m-bits instance of the computational problem then the algorithm $\mathcal{A}$ solves $\mathcal{A}(x,\ \hbar(m))$ instance.

Chapter 2

An Integrated Image Encryption Scheme Based on Elliptic Curve

The transmission of multimedia information, such as digital images, audio data, and video, via various networks significantly increased due to the rapid development in network evolution. However, mostly the data transmission procedures occurred through unsecured networks. Therefore, there is a chance that information might be lost, intercepted (i.e., copied and distributed illegally), and can be altered maliciously [19]–[22]. Over the internet, digital image is an essential source for data communication. For instance, in the medical industry, images are used for visualizing different analyses and diagnosing various diseases. These analyses are transmitted in the form of images. The patients use these images and get consultations from medical specialists anywhere around the globe. So, in this case, integrity and confidentiality violation are very dangerous for the patients.

ECC has recently been used for image encryption applications. RGB image encryption based on ECC is investigated in [13]. The presented scheme utilized DNA encoding and decoding for RGB image encryption and decryption followed by elliptic curve Diffie Hellman. The algorithm presented in [23] employed a cyclic group of an EC with the combination of chaos. In [24], Bellare and Rogaway introduced a hybrid cryptographic architecture named Elliptic Curve Integrated Encryption Scheme (ECIES). The ECIES is a pair of key-derivation functions, encryption with a symmetric key algorithm, and a Massage Authentication Code (MAC) algorithm. Since the message is sometimes difficult to encode in the points of the curve, so challenging to encrypt. Contrastingly, one can easily encrypt any message using a symmetric-key scheme of ECIES. This is a substantial benefit of ECIES over the Massey-Omura(MO) and ElGamal Public key approaches [24]. In [25], the author presented a symmetric encryption technique based on the improved version of ECIES for the application of medical images. However, the asymptotic complexity of the suggested technique is slightly increased due to the serval time of scalar multiplication of the curve points.

In view of the shortcomings above, we proposed a novel integrated image encryption algorithm in this chapter. The proposed scheme consists of a secure key exchange protocol, hash algorithm, and symmetric key algorithm. The exchange protocol is used for the communication of secret keys among the communicating parties. The hash function is used for data integrity, and the symmetric algorithm is used for data confidentiality. The confusion and diffusion module of the symmetric encryption is achieved by using simple operations that provide optimum security with less computational effort. Furthermore, the security performance of the scheme is thoroughly analyzed using the available tools. The resultant output demonstrates the scheme's efficiency compared to the existing scheme

2.1 Elliptic Curve Discrete Logarithm Problem(ECDLP)

Let $\mathbb{E}^{\mathrm{a,b}}{}_{q}$ be the elliptic curve over the finite prime field $\mathcal{F}_q$, where q is prime and $\mathrm{a, b} \in \mathcal{F}_q$. The DLP for an EC is defined as Given a points Q_1, and Q_2 on $\mathbb{E}^{\mathrm{a,b}}{}_{q}$ to find the positive integer M, if it exists, such that $Q_2 = MQ_1$ [26].

2.2 Secure Hash Algorithm

The NIST made public a category of hash functions called Secure Hash Algorithms (SHA). Applications of SHA are predominantly located in integrity security services [27]. One well-known SHA algorithm is SHA-256, which generates message digests with 256-bit lengths. The proposed algorithm generates the Hash of key of length 256-bit between users A and B. The first 128-bit is utilized for proposed symmetric key encryption, while the 128-bit length key is used for authentication.

2.3 Enhanced Elliptic Curve Integrated Encryption Scheme (E-ECIES)

The enhanced elliptic curve integrated encryption scheme E-ECIES was used to improve the secret parameter negotiation phase. The improvement of the initialization vector is to be added with the key to prevent repeated data encryption, making it harder for a hacker to detect patterns and break encryption using a dictionary attack. After that, the symmetric key encryption is extracted by the secure SHAH-256. The detailed process of the E-ECIES is summarized in the below subsection. Lets user A wants to send a plan-image M of size $\mathcal{U} \times \mathcal{V}$ to user B over the insecure channel. User B first creates his public key by choosing the EC over the finite field $\mathcal{F}_q$ of prime order that makes the discrete log problem for $EC(\mathcal{F}_q)$is difficult, and he picks a point p on EC that is generally of big prime of order $\mathcal{N}$. He then calculates the public key $P^B = \mathfrak{m}p$ using a secret number $\mathfrak{m}$. The public key parameter of user A is $\{\mathcal{F}_q,\ EC, N, p, P^B)$ while the private key of user B is $\mathfrak{m}$. The following steps are computed to transmit the data between user A and user B.

2.3.1 User A Computation

- To encrypt and send the message, user A computes the following:

- Choose a private key $n^A \in [1, q-1]$.
- Computed the public key $P^A = n^A \mathbb{G}$ with timestamp $\mathcal{T_O}^A$.
- Compute the $P^A{}_1 = n^A P^B$.
- Create a random initialization vector $\mathbb{V}$ with the increment of the prime number for every block of message, which is chosen for the private elliptic curve in the proposed symmetric key encryption function (PSKEF) to prevent the repetition throughout the encryption process; the details description of PSKEF is given in the following subsection.
- Compute the Hash to extract the symmetric key; the mathematical description of the hash function is given below.

$$Hash(P^A(x \oplus y), P^A{}_1, \mathbb{V}\ ) = H_1 = K_1||K_2 \tag{2.2}$$

- Compute the proposed symmetric key encryption function with K_1.

$$C = Enc_{K_1}(M) \text{ and } \mathcal{T} = (C, K_2)$$

- Send $< H_1, P^A, \mathcal{T_O}^A, \mathcal{T} >$ to user B.

2.3.2 User B Computation

In response to receiving the cipher image from user A, user B creates a new timestamp $\mathcal{T_O}^B$and follows the below bullets points:

- User B verifies $|\mathcal{T_O}^B - \mathcal{T_O}^A| \leq t$. If the condition does not hold user B aborts, or else he sustained. The duration of t is a short predetermined time.
- User B computes $P^A{}_1$= $\mathfrak{m}P^A$ using the knowledge of private key $\mathfrak{m}$.
- Calculate the $Hash(P^A{}_1, P^A(x \oplus y), \mathbb{V})) = H_2$. If $H_2 \neq H_1$, when it does not hold, he passes over the session. Otherwise B continues the remaining steps of the protocol.
- Generate the symmetric key $H_2 = K_1||K_2$.
- Computes $H_2(C, K_2) = \mathcal{T}_1$. If $\mathcal{T}_1 \neq \mathcal{T}$, user B rejects the cipher image; otherwise, continue the protocol steps.
- Calculate the plan-image $M = Dec_{K_1}(C)$, where Dec_{K_1} is a symmetric key decryption function. As a part of user B computation, the second last step involves authentication, which is an essential aspect.

2.4 Proposed Symmetric Key Encryption

In this section, we proposed a new symmetric key encryption algorithm based on E-ECIES. The symmetric key encryption algorithm encapsulates the following steps to perform image encryption. Initially, use secure SHA-256 to generate the key using the following mathematical formula.

$$Hash(P^{A}(x \oplus y), P^{A}{}_{1}, \mathbb{V}\ ) = \mathcal{K}_1||\mathcal{K}_2.$$

Where $\mathcal{K}_1$ followed by $\mathcal{K}_2$. To perform the encryption using key $\mathcal{K}_1$ the following steps are to be done. For the $\mathcal{K}_1 = 128\ bit$ is utilized for the encryption, while the $128bit$ of $\mathcal{K}_2$ are used for authentication purposes. Initially, the first four-byte, $b_1b_2b_3b_4$ are utilized for the permutation of the plain image using affine mapping. The mathematical construction for the permutation of the plan image using affine mapping is defined as

$$\wp: z_m \times z_m \to z_m \times z_m$$

$$\wp(\imath, \jmath) = (\imath', \jmath')$$

$$\imath' = b_1(\imath) + b_2,\ \jmath' = b_3(\jmath) + b_4. \tag{2.2}$$

Where b_1 , $b_3$the unit's elements are z_m, while, b_2 and b_4, are any elements in from z_m. The $\imath'$ and $\jmath'$, the output of the affine transformation, which shows the permuted pixel of the image.

2.4.1 Diffusion Phase Based on Elliptic Curve Pseudo-Random Number (ECPRN)

The next six bytes $b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}$ is again utilized for the permutation purpose using an elliptic curve parameter with the large prime p, which is the concatenation of the last two bytes, i.e., $p = b_{11}||b_{12}$. If the concatenation of the last two bytes is exactly not a prime number, then subtract the bytes from the concatenation last two bytes until it gets a prime number. After the generation of points on each elliptic curve, pick the y-coordinate of the first EC, i.e., $E_1^{Y_i}$, and get the first sequence, namely $\mathcal{K}_1$ Similarly, we can compute the $\mathcal{K}_2$ and $\mathcal{K}_3$ sequences by choosing the y-coordinate of $E_2^{Y_i}, E_3^{Y_i}$ respectively. After that, pick out $\mathcal{K}_1$ and $\mathcal{K}_2$ and again permute the affine permuted image A and then bit-xor with $\mathcal{K}_1$ sequence to get $S^1{}_1$, where $S^1{}_1$ represent the red channel of a permuted image. Next, choose the $\mathcal{K}_{2,}$ $\mathcal{K}_3$and permute the S and bit-xor with $\mathcal{K}_2$ to get $S^2{}_1$ where $S^2{}_1$ shows the permuted image green channel. Finally, get $S^3{}_1$ using the sequences of $\mathcal{K}_3$, $\mathcal{K}_1$ and bit-xor with $\mathcal{K}_3$. The mathematical formula for the above $\mathcal{K}_1$, $\mathcal{K}_2$ and $\mathcal{K}_1$ execution is defined as:

$$\mathcal{K}_1\ = E_1^{Y_i}: \mathcal{Y}^2 = x^3 + b_5x + b_6\ mod\ \text{p}. \tag{2.3}$$

$$\mathcal{K}_2\ = E_2^{Y_i}: \mathcal{Y}^2 = x^3 + b_7x + b_8\ mod\ \text{p}. \tag{2.4}$$

$$\mathcal{K}_3\ = E_3^{Y_i}: \mathcal{Y}^2 = x^3 + b_9x + b_{10}\ mod\ \text{p}\ . \tag{2.5}$$

Where the length of each sequence is $1 \times mn \bmod m$. The pixel scrambling and diffusion of each layer of the above affine permuted image are defined in eq(2.6-2.11)

$$A^{1}{}_{1} = A^{r}{}_{1}(\mathcal{K}_1, \mathcal{K}_2), \tag{2.6}$$

$$A^{1}{}_{1} = \mathcal{K}_1 \oplus S^{1}{}_{1}. \tag{2.7}$$

$$A^{2}{}_{1} = A^{g}{}_{1}(\mathcal{K}_2, \mathcal{K}_3), \tag{2.8}$$

$$A^{2}{}_{1} = \mathcal{K}_2 \oplus S^{2}{}_{1}. \tag{2.9}$$

$$A^{3}{}_{1} = A^{b}{}_{1}(\mathcal{K}_3, \mathcal{K}_1), \tag{2.10}$$

$$A^{3}{}_{1} = \mathcal{K}_3 \oplus S^{3}{}_{1}. \tag{2.11}$$

Concatenate all the above three-layer and get one of the permuted images.

2.4.2 Confusion Module Based on Affine Power Affine Permutation

After that, the last four-byte $b_{13}b_{14}b_{15}b_{16}$ is utilized for the confusion phase (S-box). To construct the s-box, we use affine power affine transformation (APA) [28], using the following mathematical construction.

$$S = F_2^8 \rightarrow F_2^8$$

$$S = \mathcal{A}O(\mathrm{P}O\mathcal{A}'). \tag{2.12}$$

Where, $\mathcal{A} = b_{13}(x) + b_{14}$, $\mathcal{A}' = b_{15}(x) + b_{16}$ are the affine surjection [34]. Where P still nonlinear components, which is to be defined as:

$$P(x) = x^{2^n - 2}. \tag{2.13}$$

For $n = 8$ the power polynomial becomes $\mathrm{P(x)} = x^{254}$ is a bijective permutation using any primitive polynomial in $GF(2^8)$. Moreover, the elements $b_{13}, b_{14}, b_{15}, b_{16} \in F_2^8$, so we can construct 2^{32} new APA S-box represented by $S^{a,b}{}_{c,d}$, with strong algebraic properties. The proposed APA S-box with different parameters is given in tables 7 and 8 respectively. Furthermore, we analyzed the S-box not only by the coordinate functions but also by evaluating all the security analysis by their component function and comparing it with excellent literature [29]–[37]. The comparison analysis in table 10 shows that the APA S-box has excellent algebraic properties and affine equivalent to the AES S-box [38]. Meanwhile, the only power permutation $\mathrm{P(x)} = x^{254}$, some weak properties like fixed point and opposite fixed are given in table 10, which improve by the affine parameter chosen by the proposed symmetric key extracted from the Hash of the E-ECIES. After the substitution phase, we get a cipher image. The flow diagram of the E-ECIES is illustrated in Figure 6.

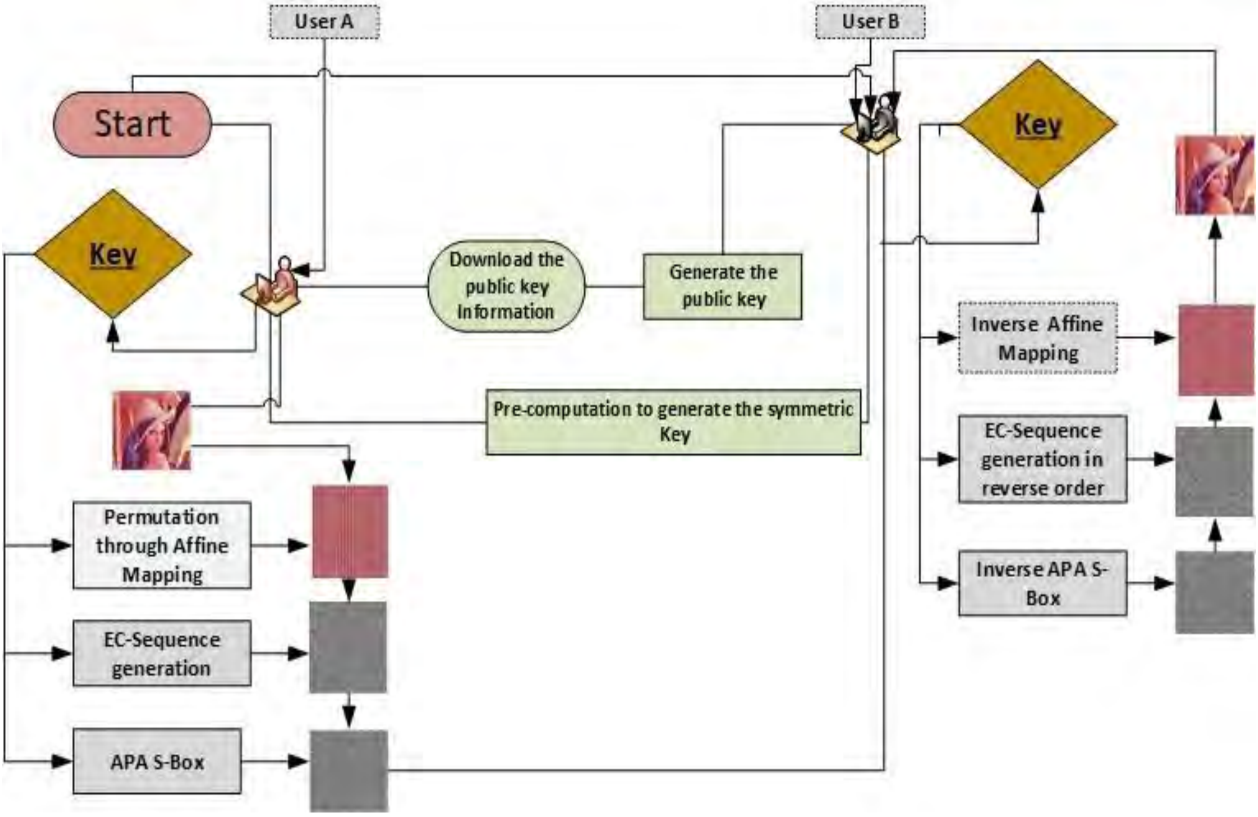

User A
User B
Start
Key
Key
Download the public key Information
Generate the public key
Pre-computation to generate the symmetric Key
Permutation through Affine Mapping
EC-Sequence generation
APA S-Box
Inverse Affine Mapping
EC-Sequence generation in reverse order
Inverse APA S-Box

Figure 6. Flow chart Proposed E-ECIES

2.5 Security Analysis of the Proposed Symmetric Key Encryption

This section compares our proposed symmetric encryption algorithm security and performance against the findings of several experiments in [13][25][29]–[37][39]–[41]. The enhanced version is subjected to several security analyses to assess the suggested work randomization and prove its resiliency against various known attacks. We take the substitution permutation network (SPN). The permutation phase is achieved by three different kinds of elliptic curves utilized for the permutation as well, as we add the nonlinear component APA S-box for the confusion phase. In the APA S-box, the encryption is evaluated by substituting uncorrelated encrypted data for plan image data. Our suggested APA S-boxes are examined using the standard S-box evaluation criteria in the results and evaluation section, which include nonlinearity score(NLS), linear approximation probability(LP), bit independence criterion(BIC), fixed point(FP), opposite fixed point(OFP), autocorrelation(AC), maximum cycle length (MCL), strict avalanche criterion(SAC), linear structure(LS), linear and differential branch number(LDBN), and differential approximation probability(DP). Moreover, in other literature[29-35], the S-box analysis is evaluated by their coordinate function, but the in our proposed work, we implement all the results on component functions well; in the case of $n = 8$, we examined $2^n - 1$, component function by their different S-box analysis. While the permutation phase evaluates the diffusion properties, including two effective tools, namely, the number of pixels change rate (NPCR) and unified average changing intensity(UACI). The portable PC with Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz 2.80 GHz is used to conduct the various evolution tests using different colored images. Figure 7 shows the suggested E-ECIES plan and corresponding encrypted images.

2.5.1 Nonlinearity Score

The nonlinearity score of function or S-box, $S = F_2{}^n \to F_2{}^m$, is represented by $\mathcal{NLS}(S)$ and defined by [42].

$$\mathcal{NLS}(S) = 2^{n-1} - \frac{1}{2}(|Walsh(\mathcal{u}, \mathcal{v})|) \tag{2.14}$$

$$S(\mathcal{u}) = \mathcal{v} \quad \text{for} \quad \mathcal{u} \in F_2{}^n, \mathcal{v} \in F_2{}^m$$

The $\mathcal{NLS}$ of APA S-box is 112, as shown in Table 10.

2.5.2 Strict Avalanche criteria

Webster and Tavares introduced the SAC idea [43]. The strict avalanche criterion (SAC) is the essential component of the S-boxes. Informally, an S-box satisfies SAC if one input bit is altered. 50% of the output bits must also be changed [43]. The mathematical description of SAC is defined in eq (2.15).

$$S = F_2{}^n \to F_2{}^m$$

$$S(x) + S(x + a) \text{ is balanced for all } a,\ wt(a) = 1 \tag{2.15}$$

2.5.3 Bit Independence Criterion

The concept of Bit independent creation(BIC) was also developed by Webster and Tavares [43]. For any two boolean functions f^i, f^j, of an S-box, if the bit-xor of both functions, i.e., $f^i \oplus f^j$, is highly nonlinear and satisfies the criterion of SAC. Then, when one input bit is changed, the correlation coefficient of each pair of output bits may be extremely near zero. So, by confirming that $f^i \oplus f^j (i \neq j)$ it holds, we may find out the BIC of the S-box of any two output bits that satisfy the SAC criterion. Table 10 shows the performance of the new APA S-box and the comparison with excellent existing literature.

2.5.4 Differential Approximation Probability

Measurement of differential uniformity is the differential approximation probability (DP) of the S-box, which is defined as:

$$\mathcal{D}p^{S}(\Delta a \to \Delta b) = \left[\frac{\neq\{a \in x|S(a) + S(a \pm \Delta a = \Delta b)\}}{2^{m}}\right] \tag{2.16}$$

Where $\Delta \boldsymbol{a}, \Delta \boldsymbol{b}$ is the input differential and output differential, which implies that an input differential $\Delta \boldsymbol{a}_i$ must precisely map to an output differential $\Delta \boldsymbol{b}_i$ Order to guarantee a uniform chance of mapping for each i. According to the Performance indexes of the new APA, the average differential approximation probability is 0.01562. The comparisons table 10 shows that the DP of the new APA S-box is better than [29][31]–[35], and the same as with AES S-box

2.5.5 Linear Approximation Probability

The linear approximation probability (LP) is the highest possible value of an event's imbalance. The mask chooses the output bits ψ_a have the same parity as the input bits chosen by the mask ψ_b. According to the Matsui mathematical formulation of linear approximation probability(LP) is defined as [44]:

$$\mathcal{LP} = \max_{\psi_a\ \psi_b \neq 0,} \left|\frac{\neq\{a \in x|a\psi_a = s(a)\psi_b\}}{2^{n}} - \frac{1}{2}\right|. \tag{2.17}$$

Where x is the set of input space and 2^n, is the total number of elements in x. The input-output masks are respectively represented by ψ_a and ψ_b Them.

2.5.6 Fixed Point

Given an S-box, $S = {F_2}^n \to {F_2}^m$, the input element $x \in {F_2}^n$ is said to be a fixed point (FP) if $S(x) = x$ [45]. The new APA S-box has no FP due to the affine transformation parameter chosen by the hash value of 128-bit in symmetric key encryption. In contrast, only the power permutation has 4 FP. The comparison table-10 shows that the new-APA S-box is on top of no fixed point like the AES S-box.

2.5.7 Opposite Fixed Point

Given an S-box, $S = {F_2}^n \to {F_2}^m$, the input element $x \in {F_2}^n$ is said to be the opposite fixed point (OFP) if $S(x) = \bar{x}$ [45]. The new APA S-box has no OFP.

2.5.8 Auto Correlation

The autocorrelation(AC) of an S-box, which is defined from, $S = {F_2}^n \rightarrow {F_2}^m$, taken concerning $\sigma \in {F_2}^n$ denoted by its polarity form $\widehat{S}$, is represented by $\widehat{r_S}(\sigma)$ and defined as [45].

$$\widehat{r_S}(\sigma) = \sum_{x \in {F_2}^n} (-1)^{S(x)+S(x+\sigma)} = \sum_{x \in {F_2}^n} \hat{S}(x) + \hat{S}(x+\sigma) \qquad (2.18)$$

The range of $\widehat{r_S}(\sigma)$ is $[-2^n, 2^n]$ for all $\sigma \in {F_2}^n$. For any n variable boolean function, the low value of autocorrelation is expected. The new APA S-box's auto-correlation value is 32, the same as the AES S-box.

2.5.9 Differential and Linear Branch Number

Given an S-box, $S = {F_2}^n \rightarrow {F_2}^m$, the differential branch number (DBN) is represented by $\varphi_{DBN}(S)$ as defined as [46]:

$$\varphi_{DBN}(S) = min_{x,x' \in {F_2}^n, x \neq x'}(\{wt(x \oplus x') + wt(S(x) \oplus S(x'))\}) \qquad (2.19)$$

The linear branch number of the S-box is denoted by $\varphi_{LBN}(S)$, and defined as:

$$\varphi_{LBN}(S) = min_{\sigma, \mathcal{B} \in {F_2}^n, \widehat{r_S}(\sigma, \mathcal{B}) \neq 0}(\{wt(\sigma) + wt(\mathcal{B})\}) \qquad (2.20)$$

Where $\widehat{r_S}(\sigma, \mathcal{B})$ shows the coefficient of autocorrelation. The suggested APA S-box the $\varphi_{DBN}(S)$ and $\varphi_{LBN}(S)$, is 2, as shown in Table 10.

2.5.10 Linear structure

The linear structure of the S-box is examined for its cryptography importance. It has been noted that attacks that could be carried out far more quickly than a thorough key search can break block ciphers with linear designs [47]. Therefore, in the block cipher, the confusion phase must avoid the linear structure. The mathematical expression of the linear structure of an S-box is defined as:

$$f(x) + f(x + a) = C \qquad (2.21)$$

Where $f(x) \in {F_2}^n \; \forall \; x \in {F_2}^n$ and for some $a \in {F_2}^n$ and $C \in F_2$. Then C is called the linear structure of the S-box. There are two types of linear structure, namely invariant if $C = 0$ and complementary if $C = 1$. Table 10 shows that the proposed APA S-box has no linear structure and is suitable for cryptographic primitives.

Table 7. Proposed APA S-box $S^{3,57}{}_{233,154}$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	139	193	16	157	237	44	218	164	153	133	112	247	27	186	141	86
2	34	151	12	145	222	221	42	61	55	89	126	229	161	143	115	179
3	166	246	29	48	134	167	10	5	163	45	3	119	38	6	99	14
4	172	192	243	108	132	136	124	67	207	140	200	100	84	146	152	189
5	30	52	235	174	116	184	131	156	95	68	220	122	203	194	96	175
6	204	57	255	76	93	137	56	11	78	228	92	97	191	213	169	91
7	190	46	138	182	98	142	87	63	197	80	252	13	0	79	28	231
8	183	154	60	244	129	1	202	82	225	173	83	73	35	201	248	121
9	144	9	114	206	230	148	25	64	69	88	49	127	113	210	181	36
10	104	59	165	118	150	242	240	65	74	195	106	40	162	226	249	232
11	77	72	158	62	53	50	253	75	188	199	4	102	160	211	155	171
12	58	205	94	19	31	216	159	250	20	128	176	7	223	47	238	214
13	90	147	2	187	26	149	180	85	254	123	110	170	178	233	43	21
14	103	251	245	24	168	120	117	22	130	101	234	33	224	66	185	239
15	51	109	212	125	135	81	196	215	15	54	208	41	23	111	107	217
16	17	70	71	39	198	177	227	105	18	241	236	219	209	37	8	32

Table 8. Proposed APA S-box $S^{2,23}{}_{1,54}$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	24	59	252	66	99	117	237	178	198	110	36	120	206	191	6	13
2	94	71	100	195	161	115	182	61	215	223	251	97	239	159	230	3
3	18	86	185	155	85	232	108	104	248	133	218	216	174	113	227	28
4	192	43	14	214	69	210	38	116	75	184	246	145	151	47	52	154
5	211	19	42	139	173	50	70	22	186	39	77	7	129	164	181	149
6	46	250	254	225	166	234	244	5	74	224	219	125	255	127	212	188
7	170	64	222	37	180	65	143	202	54	81	21	41	136	226	10	197
8	84	107	87	118	60	167	162	190	177	29	126	240	76	91	88	153
9	137	175	83	56	49	4	12	229	228	102	33	201	247	233	189	169
10	55	1	109	217	96	236	140	15	235	11	121	157	183	141	146	45
11	205	221	106	156	158	144	220	238	8	203	16	213	93	207	148	165
12	53	67	231	27	79	90	72	25	241	98	119	138	168	101	128	89
13	150	147	31	82	204	111	193	208	187	200	2	58	160	57	131	80
14	209	40	103	132	35	194	242	34	122	105	142	249	152	92	199	32
15	134	63	44	176	163	17	48	196	112	78	253	95	179	26	73	30
16	20	9	124	62	171	172	114	23	245	135	51	130	123	0	243	68

2.6 Simulation Results of Encryption

In this section, we evaluated the simulation results of the symmetric key encryption of different standard images of Lena, Apple, Babul-Quaid, and Baboon, to examine the strength of E-ECIES. The figure-7 shows the plan images listed and corresponding to their encrypted images. From figure-7 shows that the randomization of the encryption scheme is achieved. The image obtained after the encryption process reveals its unpredictability, and it is impossible to decipher the plan image without the decryption key As a result, from the simulation analysis, we identified that the original secret information could be accurately recovered without any difference or loss, proving the usefulness and validity of the entire encryption scheme.

Table 9. S-box-based on only power permutation $p(x) = x^{254}$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	203	212	40	232	176	252	39	106	138	76	237	20	220	81	24
2	1	82	218	11	79	225	27	169	222	216	36	92	42	249	236	62
3	125	65	25	111	56	3	66	108	223	59	210	18	211	67	101	46
4	160	28	89	32	52	140	102	146	145	33	98	74	175	54	72	195
5	141	123	15	163	41	229	230	4	109	114	135	5	136	154	97	34
6	246	209	228	47	192	199	172	83	50	132	191	202	159	137	23	240
7	221	205	187	53	91	104	57	69	71	147	206	38	94	166	143	251
8	156	26	119	242	35	70	243	44	244	51	231	200	22	73	184	124
9	179	227	152	162	173	235	90	168	129	208	61	87	186	151	239	113
10	30	215	21	194	207	214	241	201	130	6	118	134	60	133	31	120
11	43	180	122	197	64	63	148	157	150	131	254	49	247	155	100	37
12	153	116	7	219	255	88	139	248	115	126	29	45	2	158	167	84
13	80	78	193	48	14	13	58	85	161	182	142	188	16	121	224	117
14	93	8	10	68	198	177	110	77	250	112	165	189	181	183	12	17
15	95	75	174	226	178	204	196	144	190	127	103	105	185	149	19	9
16	96	170	99	234	238	253	213	107	86	128	55	245	164	217	171	233

Table 10. Comparison of Nonlinear component with existing algorithm

Algorithm	$\mathcal{NLS}$	AC	DP	LP	SAC	BIC	FP	OFP	LBN	DBN	LS
$\boldsymbol{p = x^{254}}$	112	32	0.0156	0.0625	0.4375	0.1285	4	1	2	2	0
$\boldsymbol{S^{2,23}{}_{1,54}}$	112	32	0.0156	0.0625	0.4375	0.1349	0	0	2	2	0
$\boldsymbol{S^{3,57}{}_{233,154}}$	112	32	0.0156	0.0625	0.4375	0.1285	0	0	2	2	0
Ref.[29]	86	120	0.2109	0.1640	0.2656	0.2887	2	3	2	2	0
Ref.[30]	112	32	0.0156	0.0625	0.4375	0.1299	1	0	2	2	0
Ref.[31]	94	96	0.0468	0.1328	0.3437	0.2799	1	1	2	2	0
Ref.[32]	94	88	0.0781	0.1484	0.3750	0.2863	1	0	2	2	0
Ref.[33]	94	88	0.0468	0.1328	0.3437	0.3069	1	1	2	2	0
Ref.[34]	94	88	0.0390	0.1328	0.3750	0.2511	2	1	2	2	0
Ref.[35]	94	88	0.0390	0.1328	0.3750	0.3138	1	0	2	2	0
Ref.[36]	94	96	0.0390	0.1328	0.3437	0.3282	2	1	2	2	0
Ref.[37]	94	104	0.0390	0.1328	0.3437	0.2204	0	1	2	2	0

2.6.1 Statistical Analysis

It is crucial to ensure that an encryption method can withstand statistical analysis when evaluating the security of the algorithms. A cryptosystem is deemed secure if it can fend off all statistical attacks. Histogram analysis, neighbouring pixels correlation, and key space play a critical role in the statistical analysis of image processing systems.

2.6.1.1 Histogram Analysis

An image's histogram can effectively and graphically depict a digital image's distribution of grey values. When the distribution of the grey value is more even, it will be more difficult for the eavesdropper to extract information from the cipher image through statistical analysis. As such, the histogram of the encrypted image should almost be uniform while differentiating itself from the one derived from the plaintext image. Moreover, the histogram's distribution was figured out from the encrypted image and is comparatively uniform, reducing the association between neighbouring pixels and preventing the attackers from learning anything. Figures 8 and 9 illustrate the histograms analysis of the plan images of Lena and Cat and their encrypted versions of Lena and Cat, respectively.

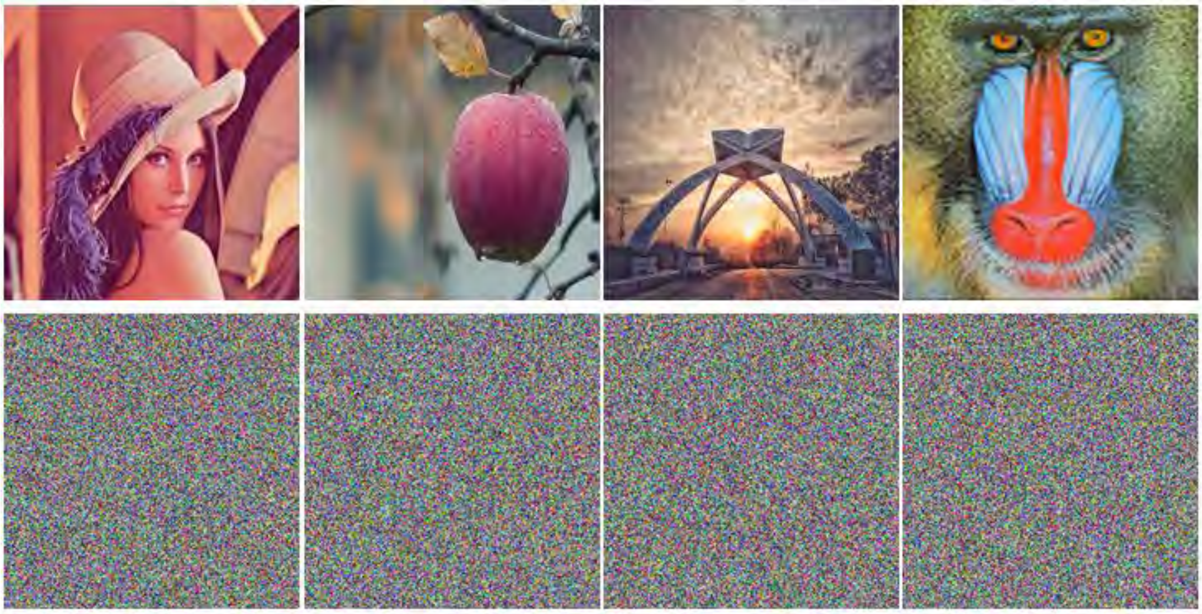


Figure 7. Row 1 shows orginal images of “Lena”, Apple, Babul-Quaid, and Baboon, and row 2 shows corresponding their Cipher Images.

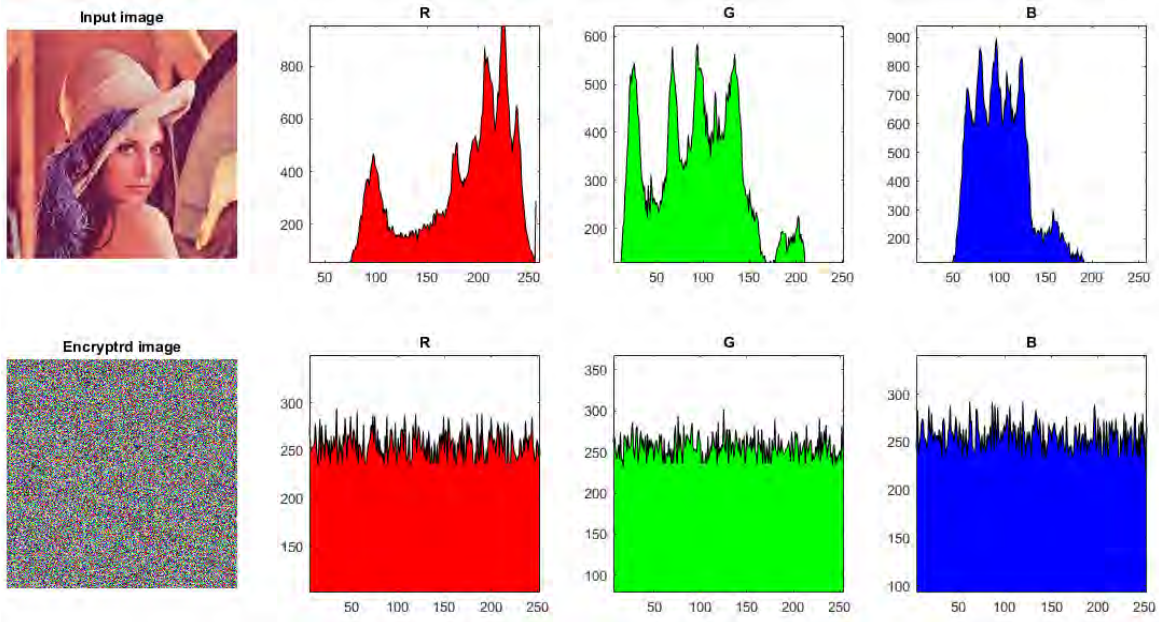


Figure 8. Histogram of original image Lena and Corresponding their Cipher image histogram

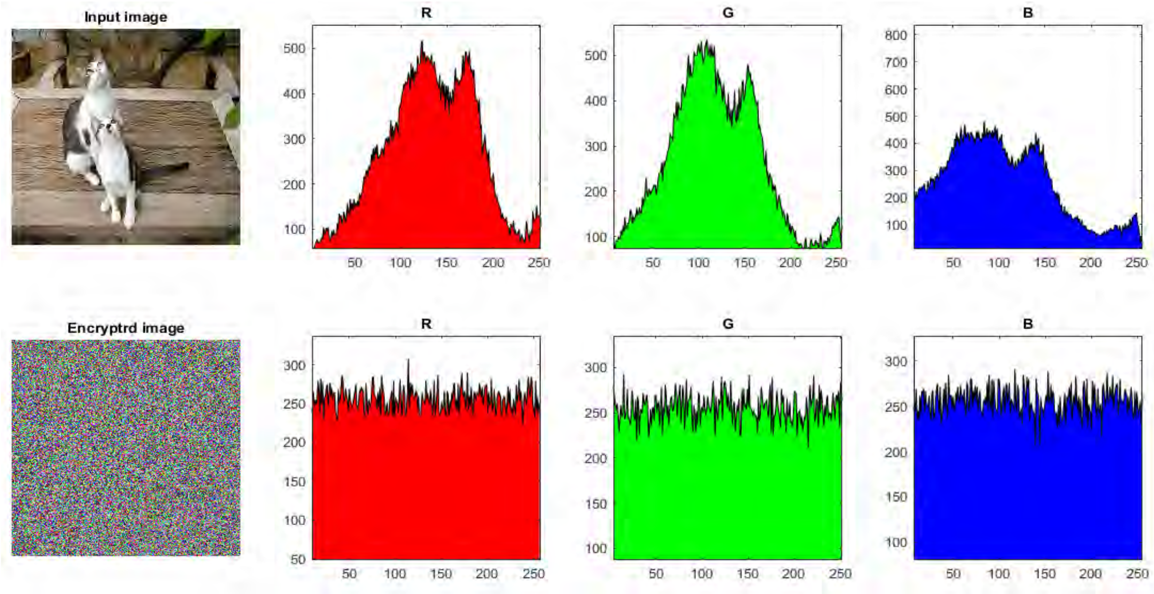


Figure 9. Histogram of original image Cat and corresponding their Cipher image histogram

2.6.1.2 Correlation Coefficent

In plaintext images, the coefficient correlation between two contiguous distinct pixels is typically significant, so a secure and efficient encryption procedure is needed to minimize this correlation. After the encypring procedure for the original images, the goal of a small coefficient correlation among the adjacent pixels should be conducted in the encrypted images. The mathematical formula for the correlation analysis between two contiguous pixels is defined as [48]:

$$\mathcal{R}(\mathbb{x}', \mathbb{y}) = \frac{\mathbb{e}(\mathbb{x} - \mathbb{e}(\mathbb{x}')(\mathbb{y} - \mathbb{e}(\mathbb{y}))}{\sqrt{\mathcal{D}(\mathbb{x}')\mathcal{D}(\mathbb{y})}}, \tag{2.22}$$

$$\mathbb{e}(\mathbb{x}') = \frac{1}{N} \sum\nolimits_{\mathbb{i}=1:n} \mathbb{x}'_{i,} \tag{2.23}$$

$$\mathcal{D}(\mathbb{x}') = \frac{1}{N} \sum\nolimits_{\mathbb{i}=1:n} (\mathbb{x}_{\mathbb{i}} - \mathbb{e}(\mathbb{x}'_{\mathbb{i}}))^2. \tag{2.24}$$

Where, $\mathbb{x}'$and $\mathbb{y}$ are the pixels of the plan and cipher image, respectively. We choose the pixel pairings in the encrypted and plaintext image in the multidirectional: Horizontal, vertical, and diagonal directions. The above eq(2.22-2.24) mathematical formula was used to get the coefficient correlation between the cipher image and the associated plaintext image in multidirectional directions. Table 11 displays the test results for the correlation in three directions between plain images and images after the encryption process. Table 11 shows that the correlation of cipher image in multidirectional is nearly close to zero, which ensures that correlation is significantly reduced. Hence, the proposed E-ECIES scheme is not vulnerable to correlation analysis.

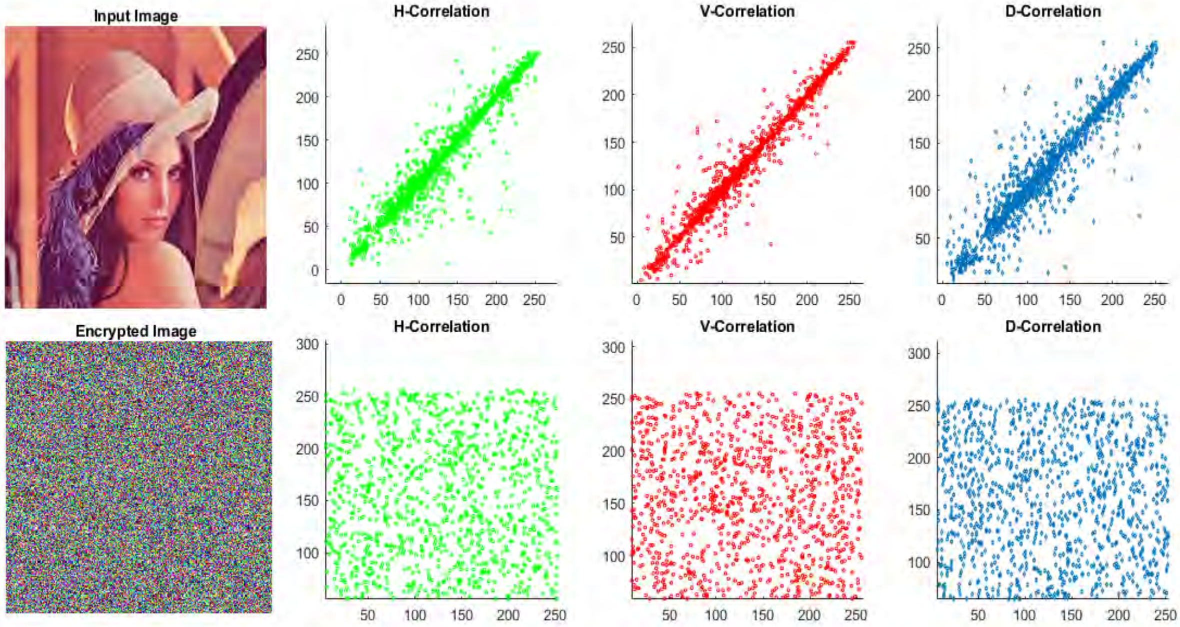


Figure 10. Correlation Analysis multidirectional (Horizontal, vertical, and Diagonal) of Plain image Lena and Corresponding their Cipher Image

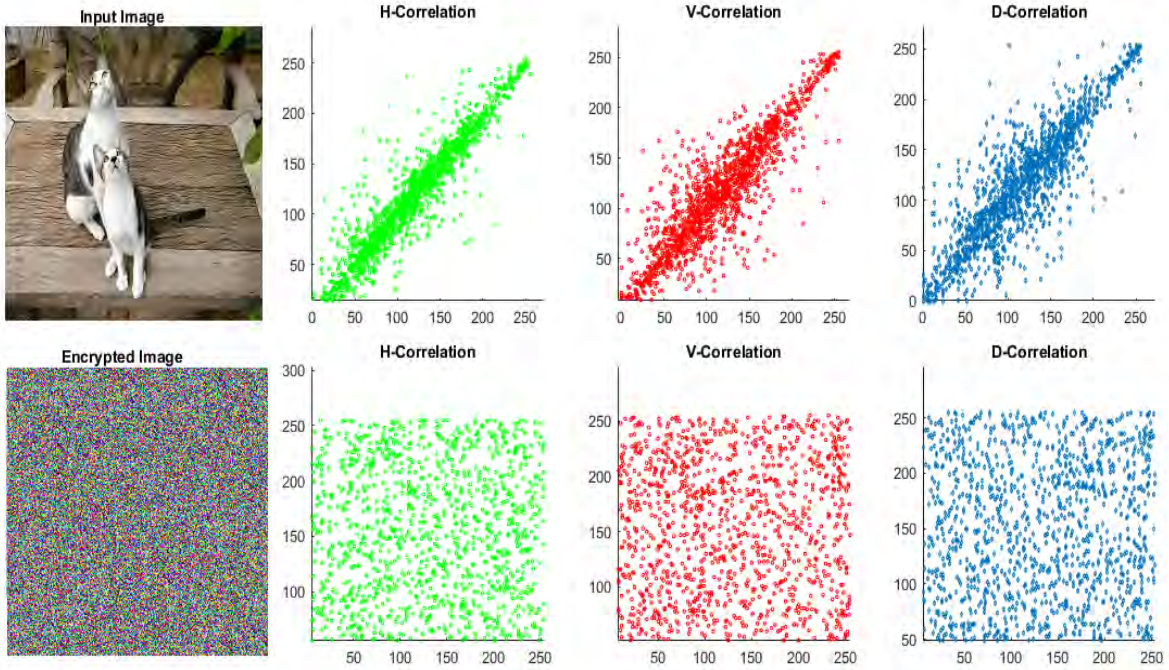


Figure 11. Correlation Analysis multidirectional (Horizontal, vertical, and Diagonal) of Plain image Cat and Corresponding their Cipher Image

Table 11. Correlation Analysis of Proposed E-ECIES

Correlation Coefficients							
		Plan-Image			Cipher-Image		
Test-Images		**H**	**V**	**D**	**H**	**V**	**D**
Lena	$\boldsymbol{R}$	0.9172	0.9504	0.9872	0.0009	0.0007	0.0007
	$\boldsymbol{G}$	0.9772	0.9618	0.9682	−0.009	−0.0009	−0.0007
	$\boldsymbol{B}$	0.9772	0.9801	0.9792	0.0017	0.0009	0.0009
CAT	$\boldsymbol{R}$	0.9801	0.9713	0.9582	−0.0219	−0.00229	−0.0229
	$\boldsymbol{G}$	0.8713	0.8456	0.9772	−0.00055	−0.0095	−0.0009
	$\boldsymbol{B}$	0.9012	0.9651	0.9372	−0.0046	−0.0046	−0.0073
Baboon	$\boldsymbol{R}$	0.9872	0.9872	0.9772	0.00021	0.0029	0.0019
	$\boldsymbol{G}$	0.9834	0.9834	0.9802	−0.0139	−0.00169	−0.0013
	$\boldsymbol{B}$	0.9751	0.9008	0.9917	0.0044	0.00049	0.0091
Babul-Quaid	$\boldsymbol{R}$	0.9026	0.9326	0.9912	−0.00319	−0.00329	−0.0075
	$\boldsymbol{G}$	0.9761	0.9861	0.9882	−0.0045	−0.0065	−0.0009
	$\boldsymbol{B}$	0.8462	0.9562	0.9698	−0.0006	−0.0026	−0.00016
Apple	$\boldsymbol{R}$	0.9636	0.9546	0.9792	−0.0009	−0.0129	−0.0079
	$\boldsymbol{G}$	0.9821	0.9701	0.9887	−0.0009	−0.0085	−0.0084
	$\boldsymbol{B}$	0.9625	0.9715	0.9917	−0.0017	−0.0016	−0.0059

2.6.1.3 Information Entropy

The information entropy, which shows the degree of confusion in the image, is one of the key characteristics of conducting the randomness of the image and evaluating the encryption method. The following equation was used to find the information entropy [25].

$$\mathbb{H}(\mathcal{m}) = -\sum_{i=1}^{\mathscr{j}} \mathcal{P}(\mathcal{m}_i) \log_2 \mathcal{P}(\mathcal{m}_i). \tag{2.25}$$

Where $\mathbb{H}(\mathcal{m})$, represent the value of entropy and $\mathcal{P}(\mathcal{m}_i)$ show the probability of $\mathcal{m}_i$. The theoretical result of the information entropy is 8. Much more uncertainty is visible, along with the image's increasing entropy. The more challenging it is for the attackers to extract information from the image, the closer it gets to the optimal value of 8. The entropy values of the Lena, Baboon, Babul-Quaid, Cat and Apple images and their corresponding encrypted images are shown in Table 12.

Table 12. Entropy Information of Proposed E-ECIES

Coefficient of Entropy							
Test-Images	Plan-Image			Cipher-Image			
	R	***G***	***B***	***R***	***G***	***B***	***Entire image Entropy***
Lena	7.2763	7.5834	7.0160	7.9972	7.9974	7.9975	7.9991
CAT	7.7450	7.7671	7.7671	7.9972	7.9972	7.9975	7.9992
Baboon	7.6094	7.3876	7.6885	7.9972	7.9974	7.9975	7.9991
Babul-Quaid	7.7600	7.6617	7.2264	7.9973	7.9973	7.9971	7.9990
Apple	7.4513	7.4170	7.2021	7.9973	7.9973	7.9971	7.9990

Concluding from the values in Table 12 that the entropy for each of the above images is close to the ideal theoretical value and utterly different from the values in the corresponding plaintext image. Considering the entropy values, we conclude that the algorithm proposed here performs effectively against the statistical attacks.

2.6.1.4 Key Space analysis

The key space shall be sufficiently large to withstand a brute-force attack. The number of keys employed in the three module namely, permutation, diffusion and confusion processes is used to compute the key space. The proposed E-ECIES initially utilized $b_1b_2b_3b_4$ for diffusion process, after that $b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}$ used for the permutation purposes and again utilized for diffusion, and the last four bytes $b_{13}b_{14}b_{15}b_{16}$ is for the confusing process. The tola number of key spaces is 2^{128} which is larger than 2^{80} and enough for brute force attacks. Moreover, the security of E-ECIES is based on the discreet logarithm problem at the initial stage of key sharing. Hence, the suggested E-ECIES has a comparatively larger key space

2.6.2 Differential Analysis

The differential attack evaluates an image encryption algorithm's plaintext sensitivity [36]. Therefore, the encryption algorithm can extend this influence over the entire encryption process if we slightly alter the plain image, a desirable image. Differential analysis is divided into two subcategories: the number of pixels change rate (NPCR) and the unified average changing intensity (UACI).

2.6.2.1 NPCR and UACI

The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are measures of the capability to withstand the differential attack. The mathematical discripation is defiend as:

$$\mathcal{NPCR} = \frac{\sum_{i=1}^{\mathcal{M}} \sum_{j=1}^{\mathcal{N}} \mathbb{F}(i,j)}{\mathcal{M} \times \mathcal{N}} \times 100\%. \tag{2.26}$$

$$\mathcal{UACI} = \frac{\sum_{i=1}^{\mathcal{M}} \sum_{i=1}^{\mathcal{N}} |\mathbb{E}'(i,j) - \mathbb{E}''(i,j)|}{255 \times \mathcal{M} \times \mathcal{N}} \times 100\%. \tag{2.27}$$

Where $\mathbb{E}'(i,j)$ is cipher image of the original image after the entire encryption process and $\mathbb{E}''(i,j)$ another encrypted image after the one-bit change in original image, both the cipher images put into the above two formulas to get the experimental analysis of $\mathcal{NPCR}$ and $\mathcal{UACI}$. Where, $\mathbb{F}(i,j)$ is defined as [25][48][44-45].

$$\mathbb{F}(i,j) = \begin{cases} 1, & \mathbb{E}'(i,j) \neq \mathbb{E}''(i,j) \\ 0, & \mathbb{E}'(i,j) = \mathbb{E}''(i,j). \end{cases} \tag{2.28}$$

Consequently, the proposed E-ECIES offers excellent resistance to the differential attack. The results $\mathcal{NPCR}$ and $\mathcal{UACI}$ measurements in this chapter and other references are also shown in Table 13. But the value of $\mathcal{NPCR}$ and $\mathcal{UACI}$ of the suggested E-ECIES is nearer to the theoretical value than for any other encryption scheme. As a result, the suggested encryption method is useful and efficient for encrypting multimedia data.

Table 13. Differential analysis

Tested images	$NPCR$			$UACI$			$Average$	
	$\boldsymbol{R}$	$\boldsymbol{G}$	$\boldsymbol{B}$	$\boldsymbol{R}$	$\boldsymbol{G}$	$\boldsymbol{B}$	$Avg\ NPCR$	$Avg\ Uaci$
Lena	99.6753	99.7531	99.6521	33.3342	33.4672	33.4192	99.6935	33.4069
Cat	99.4753	99.6521	99.6421	33.3352	33.4672	33.4192	99.5898	33.4072
Baboon	99.6753	99.6231	99.6221	33.3322	33.4442	33.4192	99.6402	33.3985
Babul-Quaid	99.6554	99.6541	99.5551	33.3352	33.4762	33.4192	99.6215	33.4102
Apple	99.6743	99.6531	99.5521	33.3372	33.4812	33.4192	99.6265	33.4125

2.6.2.2 PSNR, NC and SSIM

Three important sensitive analyses, Peak Signal-to-Noise Ratio (PSNR), Normalized Correlation ($\mathcal{NC}$), and Structural Similarity (SSIM), are used to measure the quality and change the values of pixels in images after decryption [25]. The following mathematical formula is used to compute the value of PSNR

$$PSNR = 10 \times \log_{10} \frac{2^{16} - 1}{\mathcal{MSE}}. \tag{2.29}$$

Where $\mathcal{MSE}$ is defined as:

$$\mathcal{MSE} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left(P(i,j) - E^{'}(i,j)\right)^{2}}{\mathcal{M} \times \mathcal{N}}. \tag{2.30}$$

Where $P(i,j),\ E'(i,j)$ represent the plan and encrypted receptively of size $\mathcal{M} \times \mathcal{N}$.

The similarity degree is evaluated by the normalization correlation $\mathcal{NC}$ metric. In addition, this result could be considered a reliable indicator of the encryption algorithms' effectiveness because two entirely unrelated images have a correlation coefficient that is almost zero. The equation is shown below the computed $\mathcal{NC}$ value.

$$\mathcal{NC} = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{(P(\mathscr{i},\mathscr{j}) - E'(\mathscr{i},\mathscr{j}))}{\sum_{i=1}^{m}\sum_{j=1}^{n}P(\mathscr{i},\mathscr{j})^2}. \qquad (2.31)$$

The structural similarity between the two images is evaluated using the SSIM index. This metric improves on methods like mean squared error (MSE) and conventional PSNR. On several windows of a given image, the SSIM index is calculated. As a result, the following mathematical expression provides the $SSIM$ between two windows, X and Y, of standard size $\mathcal{N} \times \mathcal{N}$.

$$SSIM(X,Y) = \frac{(2\mu_{x'}\mu_{y'} + \mathscr{b}_1)(2\sigma_{x'y'} + \mathscr{b}_2)}{(\mu_{x'}{}^2 + \mu_{y'}{}^2 + \mathscr{b}_1)(\sigma_{x'}{}^2 + \sigma_{y'}{}^2 + \mathscr{b}_2)}. \qquad (2.32)$$

where $\mu_{x'}$ and $\mu_{y'}$, shows the mean values of X and Y , respectively. $\sigma_{x'}$ and $\sigma_{y'}$, used for standard deviations of X and Y, respectively. The covariance of X and Y is represented by $\sigma_{x'y'}$, and to avoid the value of zero in dominators, the coefficients $\mathscr{b}_1$ and $\mathscr{b}_2$ are used in eq-(2.32). The comparison of the original image with the cipher image should have low $PSNR$, NC and $SSIM$ values. Otherwise, the plan and encrypted image show the value of $SSIM$ and NC is 1, and a high $PSNR$ value. Additionally, it's important to note that the image after decryption is the same as the plan image. Table 14 illustrate that the value of $PSNR$, NC and $SSIM$ of the plan-images cross-ponding their encrypted images. The results in table 15 ensure that our enhanced scheme performs well in terms of low $PSNR$, NC and $SSIM$. Finally, it can be concluded that the E-ECIES is reliable against sensitivity attacks based on the $PSNR$, NC and $SSIM$.

Table 14. PSNR, NC and SSIM values between plain and encrypted images

Security Parameters	*PSNR Values*		*SSIM*	*NC*
	P vs E	*P vs D*	*P vs E*	*P vs E*
Lena	7.8298	∞	0.0021	0.6185
Baboon	7.9832	∞	0.0131	0.7135
Cat	8.8945	∞	0.0101	0.6374
Babul-Quaid	8.5095	∞	0.0041	0.6245
Apple	9.4847	∞	0.0100	0.6588

2.6.2.3 Key Sensitivity

The secret key must be highly sensitive to an encryption technique for the actual key space to match the theoretical one. A high key sensitivity means two entirely different encrypted and decrypted outputs will arise from slightly modifying the secret key throughout the encryption and decryption procedures. We generate an original secret key K_1 utilizing the E-ECIES at random and then creating two other secret keys, $\mathcal{K}_2$ and $\mathcal{K}_3$ By modifying one bit in K_1. This process is done to determine the sensitivity of the secret keys. The original secret key K_1 and the modifying keys $\mathcal{K}_2, \mathcal{K}_3$ by the following expression.

$$K_1 = b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9 b_{10} b_{11} b_{12} b_{13} b_{14} b_{15} b_{16}$$

$$\mathcal{K}_2 = b_1 b_2 b_3 b_4 b_5 b_6 b_7 \boldsymbol{b_8} b_9 b_{10} b_{11} b_{12} b_{13} b_{14} b_{15} b_{16}$$

$$\mathcal{K}_3 = b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9 b_{10} \boldsymbol{b_{11}} b_{12} b_{13} b_{14} b_{15} b_{16}$$

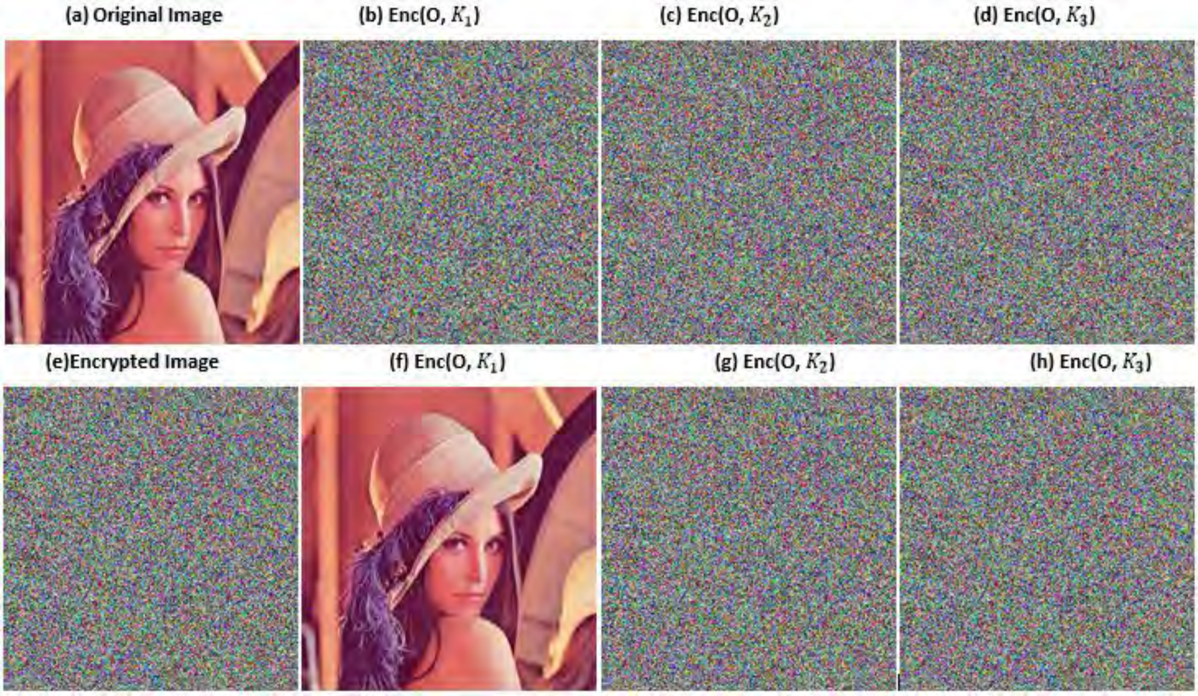


Figure 12. Key Sensitivity Analysis: 1st-row Original image Lena, Encrypt with K_1, Encrypt with K_2, Encrypt with K_3, 2nd row shows, Encrypted image of Lena, decrypted with K_1, decrypt with K_2, decrypt with K_3

Figure 12 demonstrate the results of key sensitivity, attained throughout the encryption procedure of the E-ECIES. The 1st row of Figure 12 shows the original image of Lena, three encrypted images encrypted using $K_1, \mathcal{K}_2$ and $\mathcal{K}_3$. In the 2nd row of Figure 12, only the original secret key K_1 can precisely retrieve the original image. Figure 12 illustrates how two decrypted results with just a single bit of difference between $\mathcal{K}_2$ and $\mathcal{K}_3$ they yield entirely indistinguishable results.

2.6.3 Noise Attacks

This section examines how a cryptosystem responds to noise during encryption and decryption. Some noise is always present when digital images are broadcast across communication channels. Most of the encrypted digital images are affected by different noises, and therefore, to investigate the proposed E-ECIECS, we must check the noise analysis of the suggested encryption technique and ensure that the suggested algorithm is noise resistant on this way that the digital image after decryption algorithm must be readable for the receiver sides. So, to evaluate the E-ECIECS, the cipher image is anticipated by different kinds of noise with different densities, namely: Gaussian, Salt, speckle, Poisson, and Pepper Noise. Major sources of Gaussian, Salt and Pepper, and other noise appear in remote sensing images during acquisition, including Poor illumination, high temperatures, inadequate transmission, and other factors that can all lead to sensor noise, such as electronic circuit noise [25].

2.6.3.1 Occlusion Analysis

Decryption operations for encrypted images delivered across communication channels may be ineffective due to data loss [25]. In this case, the ciphered images are subjected to a loss operation known as an occlusion attack to examine the enhanced encryption scheme noise tolerance. Figure 13 shows the encrypted colour image with data loss rates of 50% from the right and left from the top and below; similarly, 25% left and right and from top to bottom. As shown in Figure 13, after the decryption, the loss rate of 50% and 25% in an cipher image, the corresponding decipher image keeps most of the visual data from the original image. Consequently, it ensures that the E-ECIES is effective and resists occlusion attacks.

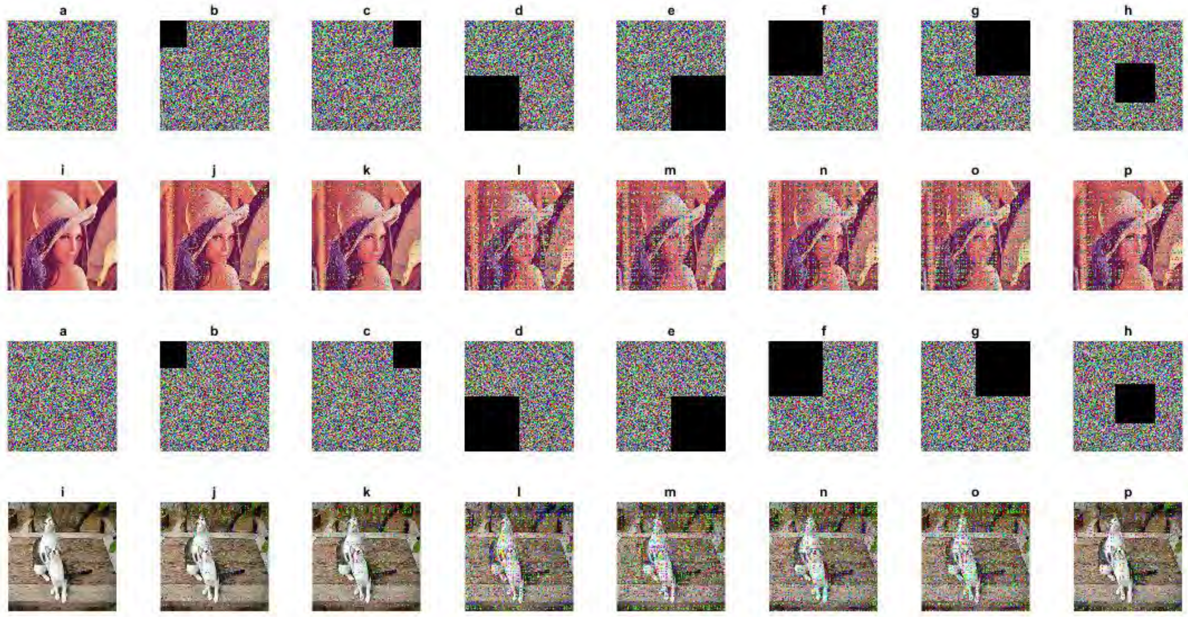


Figure 13. Occlusion Analysis 1st row from (a-h) Lena encrypted image with different rate of losing the data, 2nd row from (i-p) Crossponding Decrypted image of Lena 3rd row from(a-h) Cat encrypted image with different rate of losing the data 4th row from (i-p) Crossponding Decrypted image of Cat

2.6.3.2 Gaussian Noise

The normal distribution, which is also referred to as the Gaussian distribution, has a probability distribution function (PDF) equal to that of Gaussian noise. Additive white Gaussian noise(AWGN) is the most popular name for this type of noise [49]. The proper definition of Gaussian noise is noise with a Gaussian amplitude distribution. The following mathematical expression describes the Gaussian distribution of this kind of noise

$$\mathcal{F}(\mathscr{g}) = \frac{1}{\sqrt{2\pi\sigma^2}} - e^{(\mathscr{g}-\mathscr{m})^2}/_{2\sigma^2}. \tag{2.33}$$

Where in eq-(40), σ represents the standard deviation, $\mathscr{g}, \mathscr{m}$ shows the average and gray level of the function. For a random variable $\mathcal{S}$ of the gaussian, the PDF is expressed by the following equation eq(2.34).

$$\mathcal{PG}(\mathcal{S}) = \frac{1}{\sqrt{2\pi\sigma}} - e^{(\mathcal{S}-\mathscr{u})^2}/_{2\sigma^2}. \tag{2.34}$$

where $\mathscr{u}$ and σ represent the mean and standard deviation. The simulation results of the Lena cipher image with the addition of gaussian noise to the decrypted image of Lena in Figure 14 are still readable for the receiver side.

2.6.3.3 Salt and Pepper

Intensity spikes, often known as salt and pepper noise, are an impulsive form of noise. Generally, data transmission failures are what cause this. Each usually has a chance of less than 0.1. The image has a "salt and pepper" appearance because the contaminated pixels are alternately assigned to the minimum or maximum value. The impairment of pixel elements in camera sensors is the primary cause of the salt and pepper noise [49]. The encryption image of the suggested technique, Lena, with the addition of Salt and Pepper noise, is shown in Figure 14, along with the matching decrypted images that remain readable after the decryption procedure. By The following expression, compute the PDF for the bipolar impulse noise model

$$\mathcal{PI}(\mathcal{S}) = \begin{cases} \mathcal{P}_a & for\ \mathcal{S} = a \\ \mathcal{P}_{\mathscr{b}} & for\ \mathcal{S} \neq a \\ 0 & otherwise \end{cases} \tag{2.35}$$

2.6.3.4 Speckle Noise

A grayscale image's pixels can be affected by speckle noise, a multiplicative noise. It mainly appears in images with low brightness levels, such as MRI and Synthetic Aperture Radar (SAR) images. Before further image processing, such as object detection, picture segmentation, edge detection, etc., image enhancement is essential to reduce speckle noise [50]. Figure 14 shows the encrypted images, Lena of the proposed algorithm, with the addition of Poisson noise and corresponding decrypted images, which are still understandable after the decryption algorithm.

2.6.3.5 Poisson Noise

A random temporal distribution may be used to treat individual photon detections as separate, discrete occurrences. Thus, photon counting is a standard Poisson process. The discrete probability distribution describes the number of photons recorded by a specific sensor element across time intervals using the following mathematical formula.

$$\mathcal{P}ro(\mathcal{N} = \mathcal{K}) = \frac{e^{-\gamma\tau}(\gamma\tau)^{\mathcal{K}}}{\mathcal{K}!}. \tag{2.36}$$

This is a standard Poisson distribution with a rate parameter $\gamma\tau$ that equates to the anticipated incidence photon count, where $\gamma,$ the expected number of photons per unit of time, is proportional to the incident scene irradiance [51]. Photon noise is the term for the uncertainty that this distribution encapsulates. Photon noise offers a lower bound on the measurement error of light since it derives from the nature of the signal itself. Any measurement would be prone to photon noise even under perfect imaging circumstances, devoid of any additional sensor-based noise sources of noise (such as read noise). Figure 14 shows the encrypted images, Lena of the proposed algorithm, with the addition of Poisson noise and corresponding decrypted images, which are still understandable after the decryption algorithm. As a result, the proposed E-ECIES are secure against poison noise.

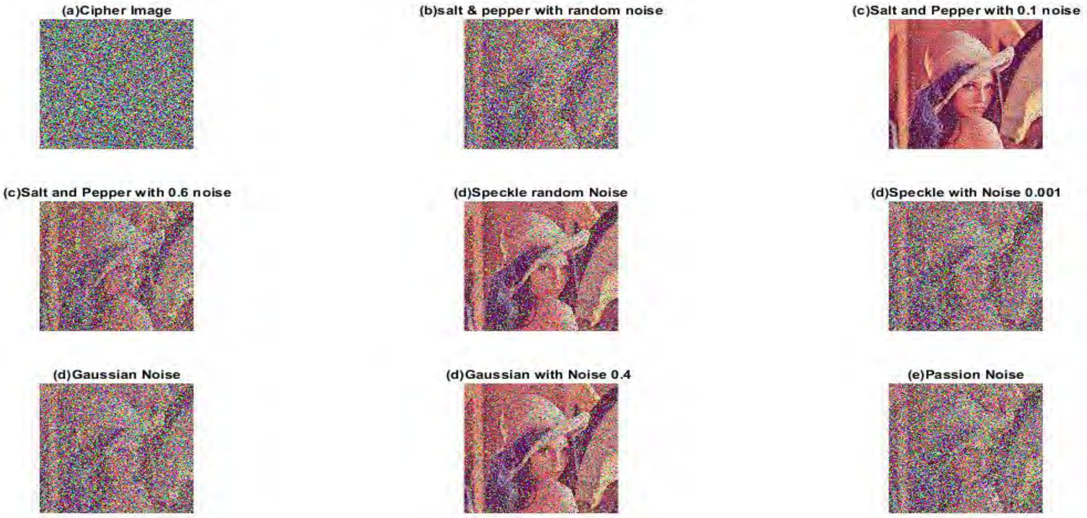

(a)Cipher Image
(b)salt & pepper with random noise
(c)Salt and Pepper with 0.1 noise
(c)Salt and Pepper with 0.6 noise
(d)Speckle random Noise
(d)Speckle with Noise 0.001
(d)Gaussian Noise
(d)Gaussian with Noise 0.4
(e)Passion Noise

Figure 14. Noise attacks: 1st-row shows (a) the encrypted image of "Lena (b) salt & pepper (0.01), (c) salt & pepper (0.1) noise.2nd row (d) speckle with random noise (d) speckle noise (0.001). 3rd- row (e) Gaussian noise (f) gaussian with 0.1 noise, and (g)passion noise

2.6.4 Computational Complexity And Running Time

The asymptotic complexity theoretically approximates the execution time of an algorithm. In general, the asymptotic complexity is denoted by big oh O. This subsection presented the proposed algorithm's asymptotic complexity and running encryption time. We have theoretically analyzed the proposed scheme's encryption and decryption procedure and skipped the preprocessing for secret key exchange. Since the proposed scheme is a substitution permutation network, in the substitution module, each byte is substituted in constant time $O(1)$. So, the complexity of the overall substitution module is $O(M \times N)$ for the image of the dimension of $(M \times N)$. Moreover, the complexity of addition and multiplication modulo n is $log(n)$ and $log(n)^2$, respectively, and the permutation module is an affine transformation that consists of addition and multiplication modulo n.

Table 15.Computational Complexity and Running Time with Other algorithms

Methode	Running time	Computational Complexity	Experimental Environment
Proposed (256*256) 1. Lena 2. Baboon 3. Cat 4. Apple	$0.2230/\text{sec}$	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
	$0.2130/\text{sec}$	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
	$0.2240/\text{sec}$	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
	$0.2250/\text{sec}$	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
Ref.[52]	$0.340/\text{sec}$	$O(7MN + 3M\log\frac{MN}{3} + 3M + 3N)$	Matlab R2017b, CPU 2.3 GHz, 8 GB memory
Ref.[53]	1.320/sec	$O(25MN)$	Matlab R2009a, CPU 2.5 GHz, 4 GB memory
Ref.[54]	$0.6212/sec$	$O(18MN + 2M\log\frac{MN}{2})$	Matlab R2012b, CPU 2.6 GHz, 2 GB memory
Ref.[55]	$0.1179/sec$	$-$	Matlab R2017, CPU 2.70 GHz, 8 GB memory
Ref.[56]	$0.38/sec$	$-$	Mathematica Version 11, CPU 1.80 GHz,1.992 MHz, 8 GB memory

So, the complexity of the permutation module is $Mlog(M) \times Nlog(N)$. So, the complexity of the overall algorithm is $M\log M^2 \times N\log N^2$. Additionally, we evaluate the proposed E_ECIES running time using Matlab R2021a. The following specifications apply to the experimental environments: Windows 10 operating system, Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM. The proposed method takes 0.2230/sec to encrypt the standard image Lena of dimension 256×256. Comparing the computational complexity and running time of the proposed E-ECIES with other existing excellent algorithms is shown in Table 15. The suggested encryption scheme performed better results compared to the [52] [53] [54] and [56] but was less effective than [55]. For evaluating encryption time, we also utilized different images of the same dimensions, 256×256. The results are displayed in Table 15.

2.6.5 Comparative analysis and discussion

In this subsection, we compared our proposed encryption algorithm with other existing cryptosystems based on EC and chose-based mathematical structures [57] [58] [59] [60] [61] [40] [30] [31] [32] [25]. The comparative analysis and discussion are based on some state-of-the-art differential and statistical analysis mentioned in Table 16. We have tested all of these metrics on a standard digital image Lena based on the proposed encryption algorithm. Image encryption techniques based on chaos, presented in [59] [60] [61] [62], are complex, have high memory requirements, and are difficult to implement on modern devices. The scheme presented [25] is based on the fusion of improved ECIES and chaotic equations, namely the Hyper chaotic Lorenz generator(HCLG) and Arnold cat map(ACT). The HCLG was utilized for the confusion module, which is unsuitable and involves more mathematical operations. They also did not properly describe the analysis of the confusion phase.

Moreover, the Cat map was utilized for the matrix multiplication, which is more expensive. While in the suggested encryption scheme, the confusion module is achieved by the nonlinear component (S-box) followed by the APA transformation. As a result, obtaining the confusion by the proposed scheme is less time-consuming than integrating the confusion and diffusion, which requires more fusion of EC and chaotic operation. Furthermore, the following bullet points give a detailed assessment of the suggested symmetric encryption algorithm with the current excellent literature.

- According to Table 16, the proposed cryptosystem outperforms in the differential analysis compared to other chaotic and EC-based encryption techniques presented in [57] [58] [31] [59] [60] [61] [62], and below from [32].
- The Entropy information of the suggested encryption is nearly close to the theoretical value and shows better results from [40][30][59][60][61], and nearly below the [57] [31] [32] [25], and equal to the [62].
- According to the correlation analysis, the results of the horizontal, vertical and diagonal of the suggested symmetric algorithm are nearly close to the theoretical value, which makes sure that the suggested encryption scheme would perform better and be resistant to statistical

attacks as compared other chaotic and elliptic curve based encryption scheme [57] [58] [39][30] [25] [59] [61] [62], and less from the [31] [32] [60].

Table 16. Comparative analysis

Security parameters	Sensitivity analysis				Statistical analysis			
Encryption method	NPCR	UACI	PSNR		H.Cor	V.Cor	D.Cor	Entropy
			P vs E	P vs D				
Proposed E-ECIES	99.6935	33.4069	7.8298	∞	0.0009	0.0007	0.0007	7.9991
Ref.[57]	99.5693	33.2824	−	−	−0.0009	0.0008	0.0021	7.9972
Ref.[58]	99.6155	33.4274	−	−	−0.0036	0.00262	0.00123	7.9995
Ref.[39]	99.7100	33.3600	8.65	∞	−0.0483	−0.0703	-0.0534	7.9995
Ref.[40]	99.3300	33.1400	−	−	0.0030	0.0050	−0.0020	7.9900
Ref.[30]	−	−	−	−	0.0081	0.0182	0.0065	7.9022
Ref.[31]	99.5911	33.3765	−	−	−0.0006	−0.0009	−0.0005	7.9994
Ref.[32]	99.976	33.5872			−0.0005	−0.0003	0.0001	7.9993
Ref.[25]	99.6541	33.4615	4.5789	−	0.0001	0.0005	0.0015	7.9993
Ref.[59]	99.6090	33.4630	−	−	− 0.0002	− 0.0070	0.0005	7.9980
Ref.[60]	99.6	33.45	9.2645	−	− 0.0003	− 0.0007	− 0.0001	7.9977
Ref.[61]	99.6418	33.5581	−	−	−0.0024	−0.0012	0.0011	7.9996
Ref.[62]	99.6053	33.4621	7.8616	∞	0.0018	−0.0042	0.0041	7.9991

- The PSNR values of the encrypted versus original image and plain versus the deciphered image of the proposed symmetric encryption are 7.8298 and ∞ respectively show better results than other cryptographic algorithms presented in [39] [60] [62], and somehow less from [25].

Based on the comparative analysis of Table 16, we can see that the proposed symmetric cryptosystem testing findings have shown better outcomes than recent chaotic and EC-based encryption techniques and give robust security and high resistance against state-of-art cryptanalysis.

Chapter 3

Mordell Elliptic Curve for Efficient Digital Audio Encryption Application

Nowadays, voice-based transmission is visible in areas like military intelligence, phone banking, secret voice conferencing, education, etc. With the increasing demand for secure audio communication, the audio encryption protocol is significant for storing and communicating sensitive data over the exposed scheme. The conventional cryptographic algorithm is not suitable for audio encryption, such as traditional algorithms like AES [63], DES [64], TDEA [65], and RSA [66] are not suitable for audio communication. The two underlying cryptographic terms, diffusion and confusion, are introduced by Claude Shannon [67]. These two terms are substitution and permutation operations achieved by random numbers or sequences. In confusion, the data value is permuted corresponding to some key parameter to dismantle the neighboring samples. However, both terms are shown a complex relation between ciphertext, plaintext, and the encryption of symmetric key algorithms; different analysts and designers use the substitution-permutation network (SPN) as a fundamental structural element [68].

Numerous encryption methods for digital audio are described in the literature. However, no one algorithm attracts the attention of all digital audio formats. In 2008 Wei-Qi Yan et al. presented a scheme of digital Audio scrambling in the compressed domain [69]. The proposed work uses scrambled digital audio data before key transmission. Nonetheless, the suggested work has not proven the security against brute force attacks [69]. Juliano B. Lima et al. suggested a digital audio encryption technique based on the cosine number transform (CNT) [70]. The anticipated approach of encryption was applicable to encrypt different blocks of audio format. The rule used to select the audio data blocks is overlapping, producing confusion and diffusion in the encrypted data. However, the computational cost of the suggested scheme is still expensive and unsuitable for large audio data. Afterward, in 2016 Hongjun Liu introduced a scheme of audio encryption by the operation of diffusion and confusion based on multi-scroll chaotic encryption and one-time keys [71]. The proposed work shows that a chaotic system with varying multi-scroll generates key streams to produce diffusion and confusion in audio data. The audio encryption technique is based on the fusion of Fast Walsh

Hadamard Transform(FWHT) and chaotic keystreams proposed by F.J. Farsana et al [72]. In the suggested work, the original audio data is permuted using a Henon Map (HM). For the second module of the encryption technique, the authors utilized the Lorenz-Hyperchaotic for keystreams generation. The computational complexity of the entire scheme is $o(n^2)$ and achieved the targeted level of security. The existing chaotic map techniques are shown to be insecure against cryptanalysis in the literature mentioned above because the one-dimensional chaotic map has fewer parameters. Moreover, techniques based on high-dimensional chaotic sequences are highly complicated, necessitating additional storage space, and most chaotic-based encryption algorithms are subject to numerous hardware limitations. This limitation is caused by the absence of mathematical non-integer operations, which require lots of space.

Considering the abovementioned issues, scholars utilized different algebraic structures to build a secure digital audio encryption scheme with infinitesimal computational cost. This chapter developed an efficient digital audio encryption algorithm with permutation-substitution architecture(PSA) using a mordell elliptic curve(MEC) with highly nonlinear components (i.e., S-box). The framework of MEC points generation utilized the searching techniques, significantly reducing the time complexity to the exceptional margin. The high-quality pseudo-random number sequences are subsequently utilized to aid the diffusion process. The phase of confusion is utilized with the help of multiple strong 5×5 S-box, which have never been applied before the existing literature. The experimental findings show that the suggested technique is effective and resistant to attacks.

3.1 Mordell Elliptic Curve

An elliptic curve over a finite field F_p, is defined as.

$$E^{\mathrm{a,b}}{}_{p} = \{\infty\} \cup \left\{(x, y): x, y \in F_p : \Upsilon^2 = x^3 + ax + b \; mod \; p\right\} \tag{3.1}$$

The particular case of EC when the parameter $a = 0$ and $b \neq 0$ is called the Mordell elliptic curve ${M_{EC}}^{0,b}{}_{p}$.

Theorem 3.1. *Let P be prime (i.e. $p > 3$) such that $p \equiv 2(mod\, 3)$. Then for each $b \in F_p$, the ${M_{EC}}^{0,b}{}_{p}$, has exactly $p + 1$ unique points. As the y-coordinate of each integer in [0, p–1] appears precisely once.*

3.2 Proposed Audio Encryption

In this section, we discuss the proposed algorithm for audio data. The proposed algorithm is to work out to secure the digital Audio in (.wav formatted) before sending it to the insecure channel. In the following steps, we briefly discuss the proposed work.

Step 1: First, read the audio file in sixteen-bit integer data whose range laying in the interval of $[2^{-15}, 2^{15}\ ]$. Reshape the original audio data in the new matrix Å of dimension $N \times N'$, where N, N', represent the rows and columns of the original audio data.

Step 2: Next, matrix Å contains non-negative and negative data in the class of signed bit integers. To identify the position of both data, the scheme creates a binary matrix β consisting of 1 and 0. The mathematical formulation of the binary matrix is given as follows.

$$\beta(i,j) = \begin{cases} 0, if \ \ \text{Å}_{i,j} < 0 \\ 1, if \ \ \text{Å}_{i,j} \geq 0 \end{cases} \tag{3.2}$$

Where $\text{Å}_{i,j}$, the data is set element of matrix Å at the $(i,j)_{th}$ position and $\beta(i,j)$ is to show the element of binary matrix β at $(i,j)_{th}$ position. Therefore, we get a binary matrix β of dimension $N \times N'$.

Step 3: Next, convert the audio data set $[2^{-15}, 2^{15} - 1]$ to $[2^{-15} - 1, 2^{15} - 1]$ to get new data set matrix $\text{Å}'$ of dimension $N \times N'$. Consequently, get the new matrix $\text{Å}'$, which contains the data values of 15 bit-digit integers. The mathematical formula for the new data set is given below.

$$\text{Å}'(i,j) = \begin{cases} \text{Å}_{i,j}, & if \ \ \text{Å}_{i,j} > 2^{-15} \\ \text{Å}_{i,j} - 1, & if \ \ \text{Å}_{i,j} = 2^{-15} \end{cases} \tag{3.3}$$

Step 4: In the next step, apply the absolute function on the data set of $\text{Å}'(i,j)$ to obtain the new data set $\text{Å}''(i,j)$ whose entries laying in the interval of $[0, 2^{15}]$. Hence the $\text{Å}''(i,j)$ transform to a 15-bit positive integer.

Step 5: Afterward, generate pseudo-random sequences using the following ${M_{EC}}^{0,b}{}_{p}$ equations eq(3.4-3.6) and pick the y-coordinates of ${E^{\Upsilon}}_1$, ${E^{\Upsilon}}_2$, ${E^{\Upsilon}}_3$ using the following mathematical expression.

$${E^{\Upsilon}}_1 = \left({M_{EC}}^{0,b}{}_{p_1}\right) mod\ N \tag{3.4}$$

$${E^{\Upsilon}}_2 = ({M_{EC}}^{0,b}{}_{p_2})\ mod\ N' \tag{3.5}$$

$${E^{\Upsilon}}_3 = \left({M_{EC}}^{0,b}{}_{p_3}\right) mod\ N'' \tag{3.6}$$

Where ${M_{EC}}^{0,b}{}_{p_1}$ ${M_{EC}}^{0,b}{}_{p_2}, {M_{EC}}^{0,b}{}_{p_3},$ are the MEC sequences with the specified modulus N, N' and N''.

Step 6: After generating sequences in step 5, a permutation with a matrix $\text{Å}''$, is performed by the proposed algorithm as a next step. Consequently, this diffusion phase aims to reduce the strong correlation among adjacent integers. The mathematical description of permutation module is defined as follows:

$$\text{Å}''^{P}(i,j) = \text{Å}''({E^{\Upsilon}}_1, {E^{\Upsilon}}_{2,}) \tag{3.7}$$

Where $\text{Å}''^{P}(i,j)$ show the integer position of permuted matrix $\text{Å}''^{P}$.

Step 7: The phase of confusion is a cryptographic approach devised to enhance the vagueness of cipher data. In this step, the proposed algorithm performed the substitution process to establish that the cipher data gives no hint regarding the original data, producing confusion in cipher data. Since, in the proposed work, the permuted data is a 15-bit positive integer so it will be computing hard to substitute the whole block of 15-bit positive data. For the sake of this purpose, the algorithm divided the block into three sub-blocks of a 5-bit positive integer using the following mathematical maps is defined as:

$$\zeta: {\mathbb{Z}_2}^{15} \longrightarrow {\mathbb{Z}_2}^{5}$$

$$\zeta(\sigma_1, \sigma_2, \dots, \dots \sigma_{14,} \sigma_{15}) \longrightarrow \zeta(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 \dots, \dots, 0,0). \tag{3.8}$$

$$\zeta_1: {\mathbb{Z}_2}^{15} \longrightarrow {\mathbb{Z}_2}^{5}$$

$$\zeta_1(\sigma_1, \sigma_2, \dots, \dots \sigma_{14,} \sigma_{15}) \longrightarrow \zeta(0,0.., \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10} \dots, 0,0). \tag{3.9}$$

and

$$\zeta_2: {\mathbb{Z}_2}^{15} \longrightarrow {\mathbb{Z}_2}^{5}$$

$$\zeta_2(\sigma_1, \sigma_2, \dots, \dots \sigma_{14,} \sigma_{15}) \longrightarrow \zeta(0,0, \dots, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}). \tag{3.10}$$

Therefore, get 3 –subblocks $\text{Å}''^{P}{}_{5_1}, \text{Å}''^{P}{}_{5_2}, \text{Å}''^{P}{}_{5_3}$, consist of 5-bit respectively.

Step 8: Generate an S-box of 5×5 using an EC over a finite field. Since the 5×5 S-box has never been utilized and evaluated before, in this chapter, we briefly mentioned the construction procedure and security analysis of 5×5 S-boxes in the next subsection.

Step 9: Then substitute the 3-subblocks $\text{Å}''^{P}{}_{5_1}, \text{Å}''^{P}{}_{5_2}, \text{Å}''^{P}{}_{5_3},$ with the 5×5 S-boxes, the substitution procedure of the subblocks is the same. Initially converts the subblocks data into binary form. Next, split the chunks of five bits of each block element into 2 and 3 bits-string and then convert a 2-bit string in the decimal range of 0 to 3(or binary 11 to 00) and 3-bit strings in the decimal range of 0 to 7 (or binary 000 to 111), then substitute each element of subblock with the element of S-box $S^{p}{}_{a,b}$. For a better explanation, read example 3.2. The mathematical representation of the substitution process is defined below.

$$\mathring{A}''^{p^{S}}{}_{5_{1}} = S^{p}{}_{a,b}\left(\mathring{A}''^{P}{}_{5_{1}}\right). \tag{3.11}$$

$$\mathring{A}''^{p^{S}}{}_{5_{2}} = S^{p}{}_{a,b}\left(\mathring{A}''^{P}{}_{5_{2}}\right). \tag{3.12}$$

$$\mathring{A}''^{p^{S}}{}_{5_{3}} = S^{p}{}_{a,b}\left(\mathring{A}''^{P}{}_{5_{3}}\right). \tag{3.13}$$

Step 10: After the phase of substitution, one can get three new subblocks $\mathring{A}''^{p^{S}}{}_{5_{1}}, \mathring{A}''^{p^{S}}{}_{5_{2}}$, and $\mathring{A}''^{p^{S}}{}_{5_{3}}$. Finally, using the xor operation and xor, the sequences of $E^{\Upsilon}{}_{3}\ mod\ 32$ with the three new subblocks obtained in step 8 to get three new encrypted data $\mathbb{C}_1$, $\mathbb{C}_2$, and $\mathbb{C}_3$ using the following mathematical formulation:

$$\mathbb{C}_1 = \left(E^{\Upsilon}{}_{3}\ mod\ 32 \oplus \mathring{A}''^{p^{S}}{}_{5_{1}}\right). \tag{3.14}$$

$$\mathbb{C}_2 = \left(E^{\Upsilon}{}_{3}\ mod\ 32 \oplus \mathring{A}''^{p^{S}}{}_{5_{2}}\right). \tag{3.15}$$

$$\mathbb{C}_3 = \left(E^{\Upsilon}{}_{3}\ mod\ 32 \oplus \mathring{A}''^{p^{S}}{}_{5_{3}}\right). \tag{3.16}$$

Step 11: To reverse the data form $\mathbb{C}_1, \mathbb{C}_2$ and $\mathbb{C}_3$ of 5-bit each block to a single 15-bit block by using the following mathematical formula:

$$\zeta^{-1}: \mathbb{Z}_2{}^{5} \times \mathbb{Z}_2{}^{5} \times \mathbb{Z}_2{}^{5} \longrightarrow \mathbb{Z}_2{}^{15}$$

$$\zeta^{-1}((\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)(\sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10})(\sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15})) \longrightarrow \left(\sigma_1, \sigma_2, \dots, \dots \sigma_{14,}\sigma_{15}\right). \tag{3.17}$$

Finally, we get a matrix $\mathring{A}_{15}{}''^{s}$ of dimension $N \times N'$.

Step 12: At the final step of the proposed algorithm map, the data set $[0\ 1\ 2, \dots, \dots 2^{15} - 1]$ of the matrix $\mathring{A}_{15}{}''^{s}$ to the data set $[-2^{15} - 1, \dots, \dots 2^{15} - 1]$, using a binary matrix defined in eq (3.18). The mathematical expression of step 12 is defined below.

$$\mathring{A}^{E}(i,j) = \begin{cases} -\mathring{A}_{15}{}''^{s}(i,j), & if\ \ \beta(i,j) = 0 \\ \ \ \mathring{A}_{15}{}''^{s}(i,j), & if\ \ \beta(i,j) = 1 \end{cases} \tag{3.18}$$

Eventually, one can get a matrix $\mathring{A}^{E}$, then convert to an audio file which is the required cipher audio file. The structural outline of the suggested encryption algorithm is demonstrated in Figure 15. We encrypted multiple audio files of varied sizes and characteristics to evaluate the proposed scheme's security. Additionally, for better understanding, the source code of the entire procedure of encryption and decryption is given in Tables 20 and 21.

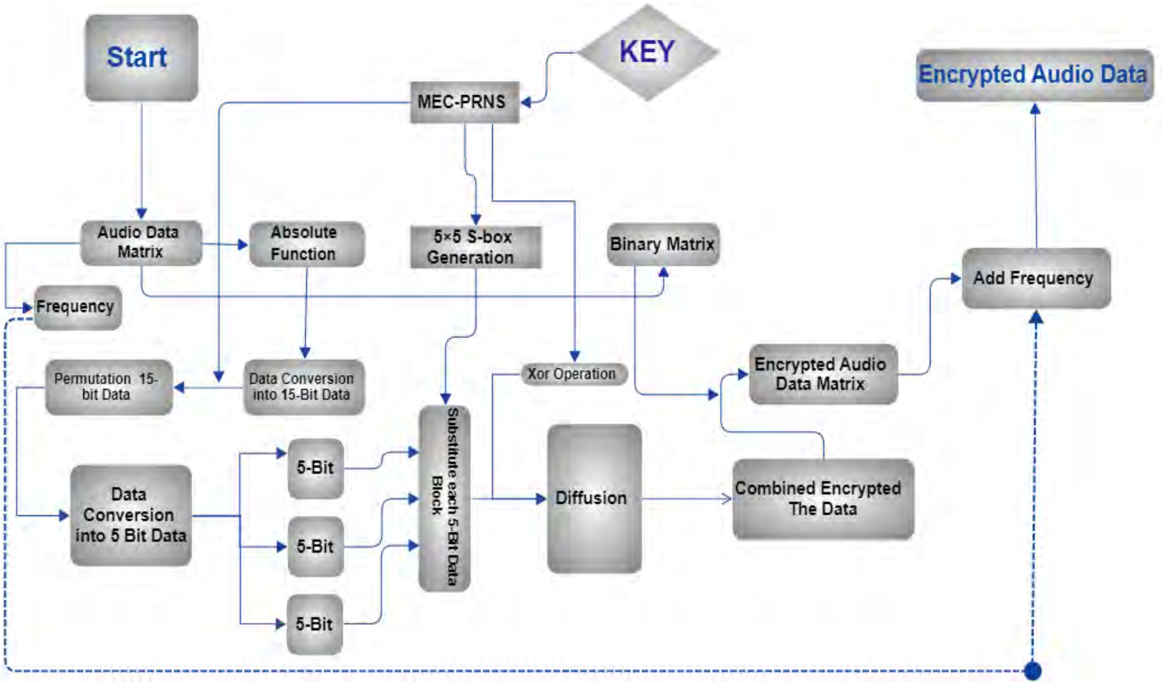


Figure 15. Flow chart of the proposed encryption scheme

3.3 5 × 5 S-box Construction and Security Analysis

Since the 5 × 5 S-box has never been applied before, the construction procedure and performance assessment of the 5 × 5 S-box are briefly covered in this section. The 5 × 5 S-boxes used to substitute three sub-blocks composed of five-bit integers are based on EC over prime fields F_p. The algorithm has four main steps described in the following steps.

Step 1: Select the domain parameters, a and b, from the prime field F_p, where p is a large prime number, i.e., $a, b \in \mathrm{F}_p, a \neq b$.

Step 2: Next, our approach to generating EC points using the searching method reduces the complexity to a significant extent. The following Weierstrass cubic elliptic curve utilizes to generate the points.

$$E^{\mathrm{a,b}}{}_p = \Upsilon^2 = x^3 + ax + b \; mod \; p$$

Step 3: Afterward, pick the ϒ-coordinate $E^{\mathrm{a,b},v_i}{}_p(u_i, v_i)$ of all orders paired $E^{\mathrm{a,b}}{}_p(u_i, v_i)$, then apply the modulo 32 operation on $E^{\mathrm{a,b},v_i}{}_p(u_i, v_i)$ to get the $E^{\mathrm{a,b},v_i}{}_{32}(u_i, v_i)$. The aim of modulo 32 is to substitute the three sub-block each of five-bit integer data. The mathematical formulation of this step is given below.

$$\partial : F^8{}_2 \rightarrow F^5{}_2$$

$$\partial: E^{\mathrm{a,b}}{}_{p} \rightarrow E^{\mathrm{a,b}}{}_{p'}$$

$$\partial(u, v) = v \; mod \; (p') \tag{3.19}$$

Step 4: In the final step, we choose the first 32 unique elements of $E^{\mathrm{a,b},v_i}{}_{32}(u_i, v_i)$to generate an s-box $S_{a,b}^{p'}$, and transmute into a 4×8 lookup table.

The implementation of the suggested algorithm is demonstrated on different ECs with distinct parameters for the generation of keyed S-boxes. Three different S-boxes $S_{1,1}^{32}$, $S_{1,3}^{32}$ and $S_{0,1}^{32}$ are generated by $E^{1,1}{}_{211}, E^{1,3}{}_{197}$ and $E^{0,1}{}_{293}$ respectively shown in Tables 17,18 and 19.

Table 17. Proposed 5×5 $E^{1,1}{}_{211}$ S-box

	0	1	2	3	4	5	6	7
0	2	13	22	29	5	15	30	16
1	4	14	24	0	6	21	31	19
2	8	17	25	1	10	23	7	26
3	12	18	28	3	11	27	9	20

Table 18. Proposed 5×5 $E^{1,3}{}_{197}$ S-box

	0	1	2	3	4	5	6	7
0	3	9	20	28	4	18	14	31
1	5	10	21	29	12	26	23	1
2	6	11	24	0	15	30	8	27
3	7	16	25	2	17	13	22	19

Table 19. Proposed 5×5 $E^{0,1}{}_{293}$ S-box

	0	1	2	3	4	5	6	7
0	3	24	12	22	11	20	9	8
1	2	13	25	15	26	17	28	29
2	14	18	31	16	30	27	4	0
3	23	19	6	21	7	10	1	5

Example 3.2. Let the input data $\mathrm{I} = (21)_{\mathrm{x}} = (10101)$ of the S-box, i.e $\mathrm{S}_{1,3}^{32}$, then the $\mathrm{outer_{bits}}(11)$ identify row 3 while the $\mathrm{inner_{bits}}(010)$ represent column 2. The numbering of rows and columns start from 0 to 3 and 0 to 7, respectively. If we substitute the input data I with the S-box, i.e $\mathrm{S}_{1,3}^{32}$, then the return byte of the S-box is $\mathrm{S}_{1,3}^{32}(21) = 25$.

3.4 Security analysis of 5×5 S-box

In the given subsection, we present some algebraic and probabilistic analyses of the suggested S-boxes based on the EC over a finite field, as shown in Table 22. The suggested S-boxes review further by performance analyses like Nonlinearity (NL), Bic independent criteria (BIC), Strict Avalanche criteria (SAC), linear approximation portability (LAP), and Differential approximation probability (DP), which is already discussed in chapter 2. The mathematical expression $2^{(N-1)} - 2^{(\frac{N-1}{2})}$, calculates the upper bound NL of the proposed s-boxes. Thus, in our case, for $N = 5$, the optimum nonlinearity value is 12. The average score of nonlinearities of the new design s-boxes $S_{1,1}^{32}$, $S_{1,3}^{32}$ and $S_{0,3}^{32}$ given in Table 22 are $10,$ which is close to the upper bound value. Similarly, the security analysis results, SAC, BIC, DP, and LP, have been presented in the same table, proving that the suggested S-box is unaffected by all possible algebraic and statistical attacks.

Table 20. Source Code of Audio Encoding

```
$O = Original\ audio\ data$ ;
$Output = Encrypted\ audio\ data$
$F \leftarrow Frequency;$
$[O, F] \ \leftarrow read\ (O,'\ native');$
$[m, n] \ = size(O);$
$L \rightarrow Length\ (m, n);$
%Sequence generation
$for\ i = 1\!:\!L\ do$
$E^{\Upsilon}{}_1 \leftarrow M_{EC}{}^{0,b}{}_{p_1}$
$E^{\Upsilon}{}_2 \leftarrow M_{EC}{}^{0,b}{}_{p_2}$
$E^{\Upsilon}{}_3 \leftarrow M_{EC}{}^{0,b}{}_{p_3}$
End
% Binary matrix generation
$for\ i = 1\!:\!m\ do$
$for\ j = 1\!:\!n\ do$
$\beta(i, j) = 1$
$if\ \mathring{A}_{i,j} \geq 0$
$else$
$\beta(i, j) = 0$
$end$
$end$
$\mathring{A}''$ =Abs ($\mathring{A}$)
% Data conversion
$for\ i = 1\!:\!m\ do$
$for\ i = j\!:\!n\ do$
$if\ \ \mathring{A}_{i,j} > 2^{-15}$
$\mathring{A}(i, j) = \mathring{A}_{i,j};$
$else\ \mathring{A}_{i,j} = 2^{-15}$
$\mathring{A}(i, j) = \mathring{A}_{i,j} - 1;$
% Difusion phase
$for\ i = 1\!:\!m\ do$
$for\ i = j\!:\!n\ do$
$\mathring{A}''^{P}(i, j) = \mathring{A}''(E^{\Upsilon}{}_1 , E^{\Upsilon}{}_2 ,)$
$end\ \ end$
% Generation of S-box
$S_{1,1}^{32} \leftarrow E^{1,1}{}_{211};$
$S_{1,3}^{32} \leftarrow E^{1,3}{}_{197};$
$S_{0,1}^{32} \leftarrow E^{0,1}{}_{293};$
% Five-bit shifting
$\mathring{A}''^{P}{}_{5_1} \leftarrow \ \mathring{A}''^{P}$ $-bitshift(bitshift(\mathring{A}''^{P}, -\mathbf{5}),5);$
$\mathring{A}''^{P}{}_{5_2},$ $\leftarrow bitshift(bitshift(\mathring{A}''^{P}, -\mathbf{5}),5);$
$\mathring{A}''^{P}{}_{5_3}$ $\leftarrow bitshift\ (bitshift\ (\mathring{A}''^{P}, -\mathbf{5}),5).$
% Substitution phase
$\mathring{A}''^{p^S}{}_{5_1} \leftarrow S_{1,1}^{32}(\mathring{A}''^{P}{}_{5_1})$
$\mathring{A}''^{p^S}{}_{5_2} \leftarrow S_{1,3}^{32}(\mathring{A}''^{P}{}_{5_2})$
$\mathring{A}''^{p^S}{}_{5_3} \leftarrow S_{0,1}^{32}(\mathring{A}''^{P}{}_{5_3})$
% Bit-xor operation
$\mathbb{C}_1 \leftarrow (E^{\Upsilon}{}_3\ mod\ 32 \oplus \mathring{A}''^{p^S}{}_{5_1})$
$\mathbb{C}_2 \leftarrow \left(E^{\Upsilon}{}_3\ mod\ 32 \oplus \mathring{A}''^{p^S}{}_{5_2}\right)$
$\mathbb{C}_3 \leftarrow (E^{\Upsilon}{}_3\ mod\ 32 \oplus \mathring{A}''^{p^S}{}_{5_3})$
$\mathring{A}_{15}{}''^{s}\ (i, j) \leftarrow \mathbb{C}_1 \oplus \mathbb{C}_1 \oplus \mathbb{C}_1$
% Reverse conversion
$for\ i = 1\!:\!m\ do$
$for\ i = j\!:\!n\ do$
$if\ \ \beta(i, j) \geq 0$
$\mathring{A}_{15}{}''^{s}\ \leftarrow\ \mathring{A}^{E}(i, j)$
$else$
$\mathring{A}_{15}{}''^{s}\ \leftarrow\ -\mathring{A}^{E}(i, j)$
$end\ ; end; end$
audiowrite (‘encryptedata.wav ’, $\mathring{A}_{\mathbf{15}}{}''^{s}$ ,$\boldsymbol{F}$)
```

Table 21. Source Code of Audio Decoding

```
$Input$ →Encrypted audio data
output→ plain audio data
[E, F] ←read (E,’ native’);
F←Frequency;
[m, n] =size(E);
L←length(m, n);
$Å_{\mathbf{15}}{''}^{s} = \boldsymbol{E}$;
% Binary matrix generation
$for\ i = 1{:}\ m\ do$
$for\ j = 1{:}\ n\ do$
$\beta(i,j) = 1$
$if\ Å_{15}{''}^{s} \geq 0$
$else$
$\beta(i,j) = 0$
$end$
$end$
$Å'' =$Abs (Å)
% Data conversion
$for\ i = 1{:}\ m\ do$
$for\ i = j{:}\ n\ do$
$if\ \ Å_{i,j} > 2^{-15}$
$Å(i,j) = Å_{i,j}$;
$else\ Å_{i,j} = 2^{-15}$
$Å(i,j) = Å_{i,j} - 1$;
% Five-bit shifting
$Å''^{P}{}_{5_1}$ ←bitshift(bitshift($Å''^{P}$, −5),5);
$Å''^{P}{}_{5_2}$,←bitshift(bitshift($Å''^{P}$, −5),5);
$Å''^{P}{}_{5_3}$ ←bitshift(bitshift($Å''^{P}$, −5),5);
% Generation of inverse S-box
$S_{1,1}^{32} \leftarrow inv(E^{1,1}{}_{211})$;
$S_{1,3}^{32} \leftarrow inv(E^{1,3}{}_{197})$;
$S_{0,1}^{32} \leftarrow inv(E^{0,1}{}_{293}$
% Re-substitutions phase
$Å''^{p^S}{}_{\mathbf{5_1}} \leftarrow \boldsymbol{S_{1,1}^{32}}(Å''^{P}{}_{\mathbf{5_1}})$
$Å''^{p^S}{}_{\mathbf{5_2}} \leftarrow \boldsymbol{S_{1,3}^{32}}(Å''^{P}{}_{\mathbf{5_2}})$
$Å''^{p^S}{}_{\mathbf{5_3}} \leftarrow \boldsymbol{S_{0,1}^{32}}(Å''^{P}{}_{\mathbf{5_3}})$
% Inverse Sequence generation
$for\ i = 1{:}\ L\ do$
$E^{\Upsilon}{}_{1} \leftarrow inv(M_{EC}{}^{0,b}{}_{p_1})$
$E^{\Upsilon}{}_{2} \leftarrow inv(M_{EC}{}^{0,b}{}_{p_2})$
$E^{\Upsilon}{}_{3} \leftarrow inv(M_{EC}{}^{0,b}{}_{p_3)}$
end
% Bit-xor operation
$\mathbb{C}_1 \leftarrow (E^{\Upsilon}{}_3\ mod\ 32 \oplus Å''^{p^S}{}_{5_1})$
$\mathbb{C}_2 \leftarrow \left(E^{\Upsilon}{}_3\ mod\ 32 \oplus Å''^{p^S}{}_{5_2}\right)$
$\mathbb{C}_3 \leftarrow (E^{\Upsilon}{}_3\ mod\ 32 \oplus Å''^{p^S}{}_{5_3})$
$Å_{15}{''}^{s}(i,j) \leftarrow \mathbb{C}_1 \oplus \mathbb{C}_1 \oplus \mathbb{C}_1$
% Difusion phase
$for\ i = 1{:}\ m\ do$
$for\ i = j{:}\ n\ do$
$Å''(i,j) = Å_{15}{''}^{s}(E^{\Upsilon}{}_{1}, E^{\Upsilon}{}_{2},)$
$end\ \ ; end$
% Reverse conversion
$for\ i = 1{:}\ m\ do$
$for\ i = j{:}\ n\ do$
$Å_{i,j} \leftarrow Å''(i,j)$
$if\ \ \beta(i,j) \geq 0$
$else$
$Å_{i,j} \leftarrow -Å''(i,j)$
$end\ ; end; end$
audiowrite(‘ original data.wav ’, $Å_{i,j}$, F)
```

Table 22. Security analysis of proposed 5 × 5 S-boxes

S-box	**NL**	**SAC**	**BIC**	**SAC-BIC**	**LP**	**DP**	**LBN**	**DBN**	**LS**
Proposed $\boldsymbol{S_{1,1}^{32}}$ (5 × 5)	10	0.527	0.600	0.5250	0.25	0.25	2	2	0
Proposed $\boldsymbol{S_{1,3}^{32}}$ (5 × 5)	8	0.5124	0.6181	0.5250	0.3125	0.25	2	2	0
Proposed $\boldsymbol{S_{0,1}^{32}}$ (5 × 5)	8	0.5122	0.5222	0.4625	0.25	0.1875	2	2	0
Ref.**[73]**. S-box (**8** × **8**)	108	0.4988	52.851	0.4988	−	-	2	2	0
Ref.**[32]**. S-box (**8** × **8**)	107	0.4990	−	0.50635	0.03906	0.1250	2	2	0
Ref.**[74]** S-box (**7** × **7**)	52	0.4978	52.851	0.504	0.09375	0.0156	2	2	0
Ref **[75]**. S-box (**4** × **4**)	4	0.4922	−	0.2500	0.2500	0.0625	2	2	0

3.5 Security analysis of Audio encryption

Effective multimedia data encryption should be robust enough to fend off all attacks, namely statistical, brute-force, eavesdropping, and other cryptanalytic approaches. Throughout part of this section will examine how the proposed encryption scheme is vulnerable to several types of attacks. Matlab 2021(a) uses a portable PC to conduct the simulations. To analyze the suggested scheme, we selected a number of audio samples with different characteristics, including voice, music, etc., and then encrypted them using different elliptic curve key parameters. Figure 16 illustrates the waveforms of the plain audio and encrypted audio files. The amplitude depicted in the cipher audio is uniform. It resembles the amplitude of the plan audio data, proving that the audio data has been effectively encrypted, as shown in Figure 16. Afterward, we will study the scheme with various analyses, such as spectrogram, histogram, entropy, correlation, and differential analysis discussed in chapter 2. Therefore, in this section, some analysis is just shown by their graphical illustrations, not their theoretical description.

3.5.1 Histogram analysis

The histogram analysis examines the proposed audio encryption-based SPA using MEC. The result of the histogram analysis is illustrated in Figure 17. Figures 17 shows the histogram of plain and cipher audio data, respectively. As observed, the histogram of plan audio data is randomized and approaches a fixed location. On the other hand, the histogram of cipher audio data nearly resembles each other. As a result, the recommended audio encryption algorithm is exceptionally secure against statistical attacks, and Eve could not decrypt the cipher data.

3.5.2 Spectrogram analysis

The spectrogram analysis is an accurate and visual representation of audio data and is the tool for analyzing sound data. A spectrogram is a standard two-dimensional plot in which one axis represents the time domain. In contrast, the axis visualizes the frequency with the colour of each point indicating its amplitude. As a result, a spectrogram shows amplitude variations for each signal frequency component. To evaluate the recommended encryption scheme, we used spectrogram analysis. The spectrogram graph analysis of the proposed audio encryption algorithm demonstrates in Figure 18. Form Figure 18 shows the analysis of the original audio data, while the second column of Figure 18 shows the spectrogram graph of the cipher audio data. Moreover, from Figure 18, one can determine that the spectrogram analysis of the encrypted audio is flat, has a considerable amplitude, and is different from the spectrogram graph of the plan audio data, ensuring that the digital audio data has been effectively encrypted.

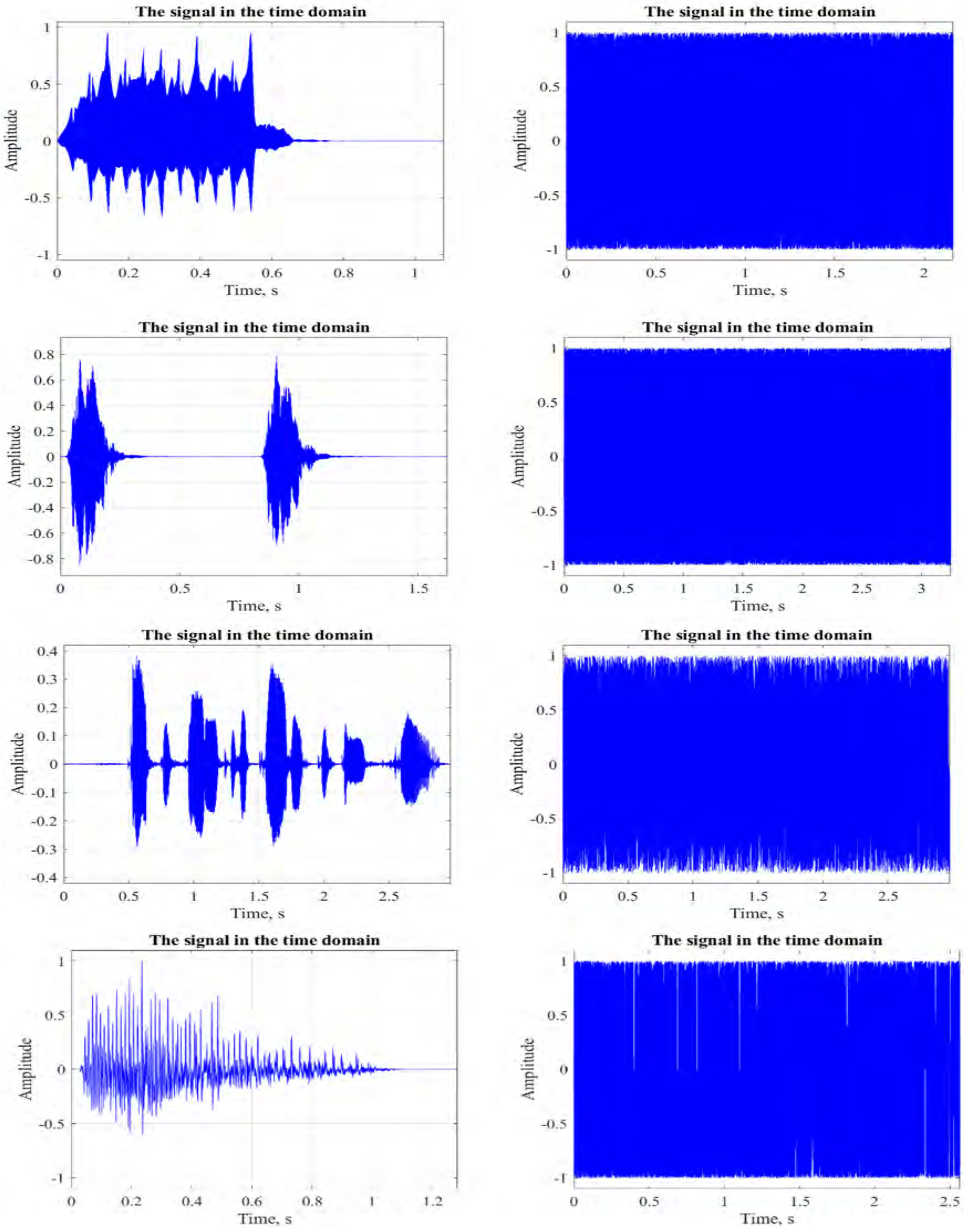


Figure 16. The first column shows the Waveforms of the original audio Alarm, female, baby and explosion. The second column shows corresponding their encrypted audio

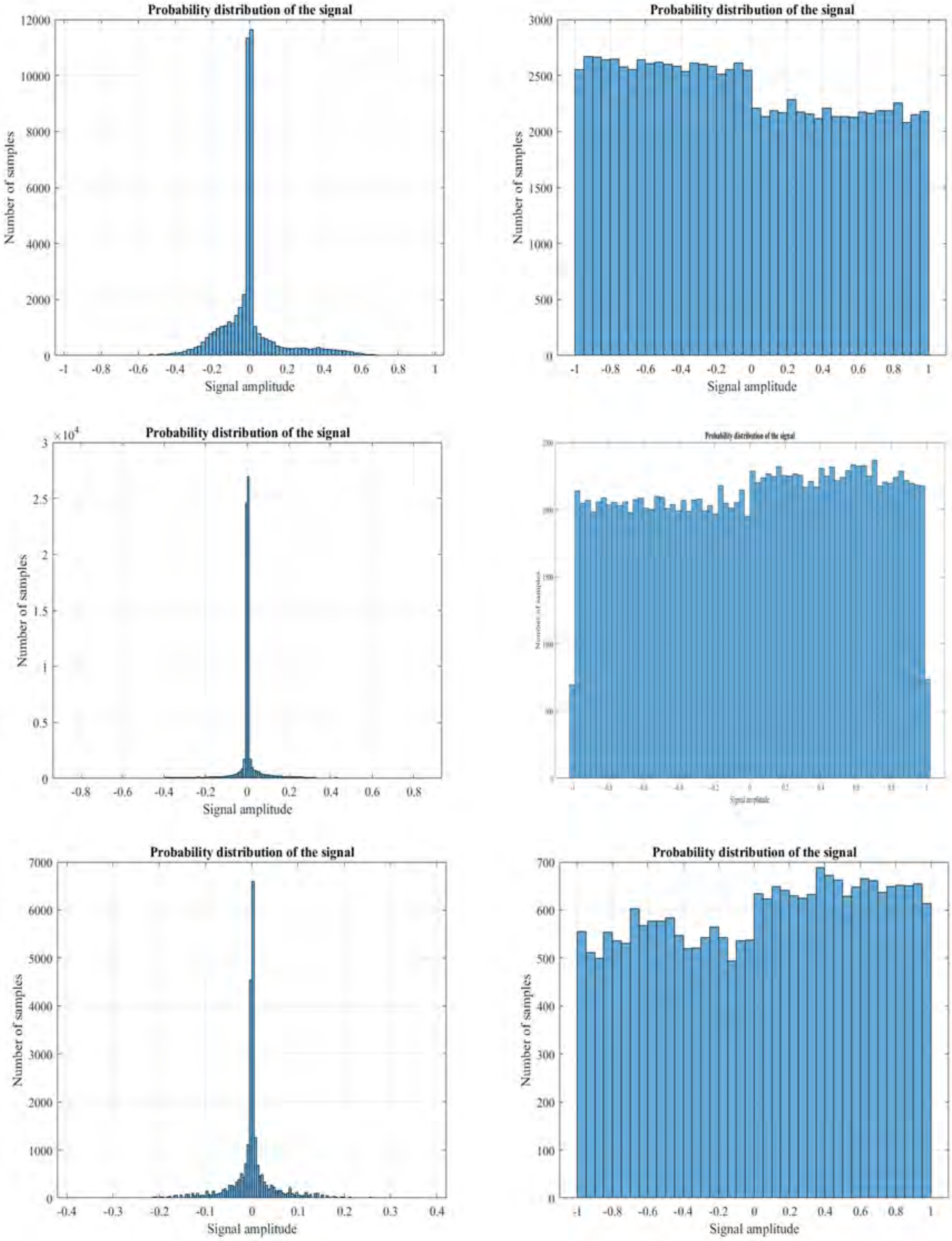


Figure 17. The first column shows the Histogram analysis of the original audio of the Alarm, female and baby, respectively. The second column is there corresponding encrypted audio histograms.

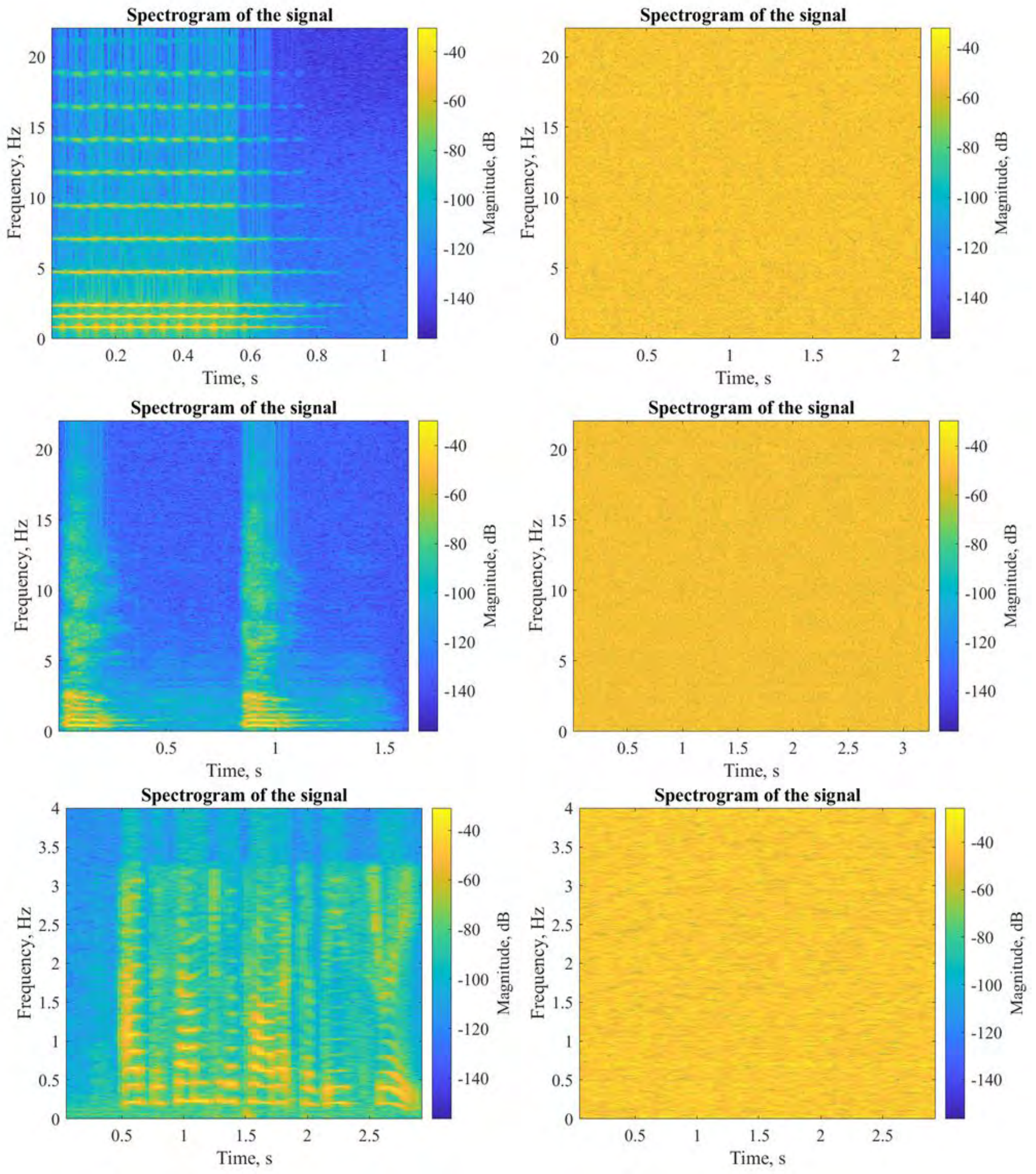


Figure 18. The first column shows the Spectrogram analysis of the original audio of the Alarm, female and baby, respectively. The second column is there corresponding encrypted audio histograms

3.5.3 Correlation analysis

We test the suggested audio encryption scheme by correlation analysis. Generally, correlation analysis evaluates the data in multiple directions, such as horizontal, vertical, and diagonal. Since the sample of audio data is highly correlated with one another. Therefore, a highly secured cryptosystem should break the correlation between audio data samples. Therefore, we picked different adjacent samples to examine the correlation coefficient in multiple dimensions. After all, the audio data samples are organized in a single array of strings, so we investigate the analysis of the correlation of the suggested scheme in the horizontal dimension. The result is summarized in Table 23. Table 23 shows that the coefficient of correlation for the plan audio data is 1, indicating that the audio data segments are highly associated.

Nevertheless, the results of encrypted audio data are nearly equal to zero, which shows that the recommended encryption algorithm disrupts the highly connected audio segments. Furthermore, the plan and encrypted audio data analysis is illustrated in Figure 19. From Figure.19, we can observe that the proposed encryption scheme is highly resistant to statistical attacks.

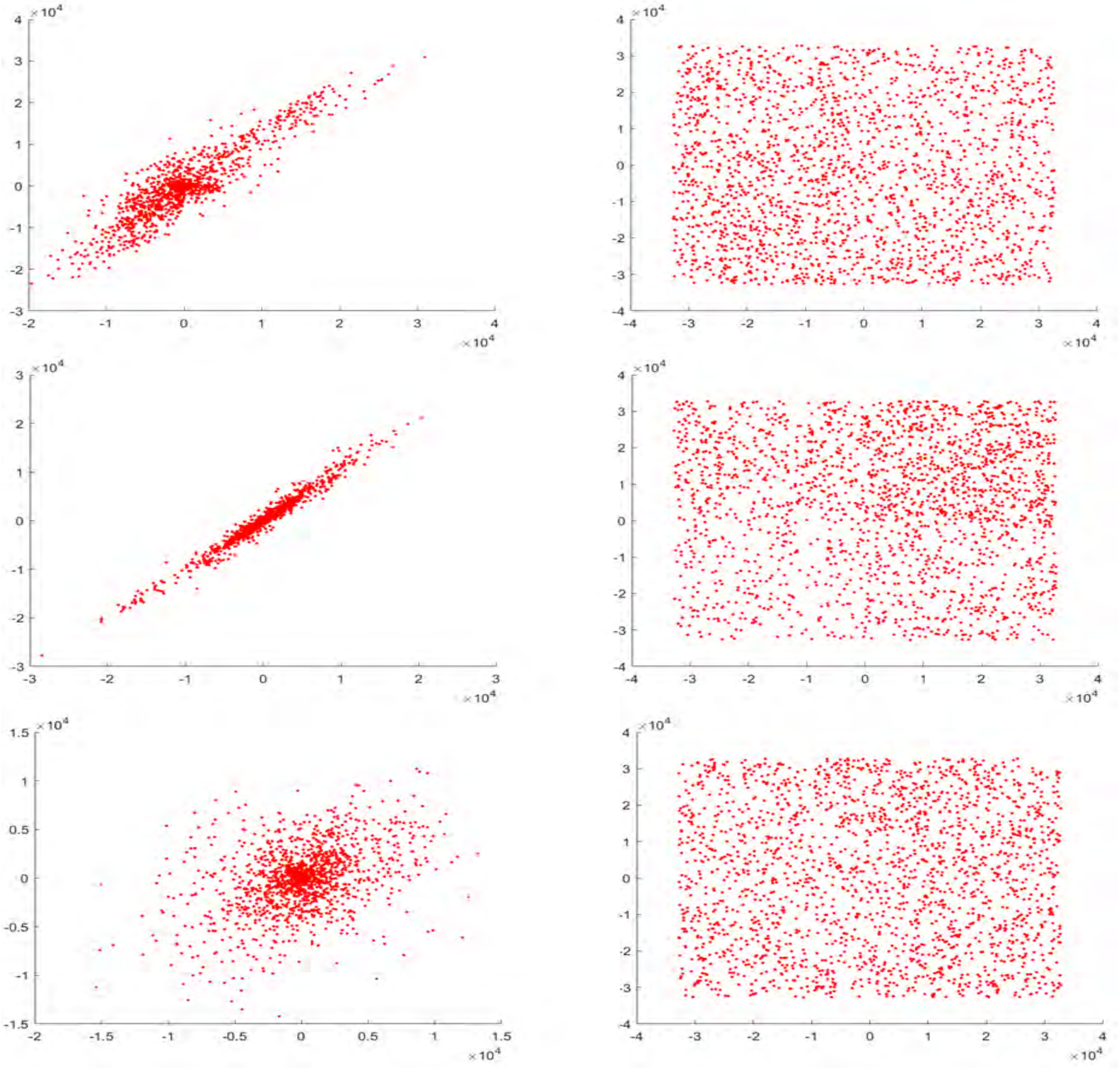


Figure 19. First column shows the Correlation analysis of the original audio of the Alarm, female and baby, respectively. Second column are there corresponding encrypted audio histograms

Table 23. Correlation analysis of various samples Audio

S.no	Audio samples	Size/KB	Plain Audio	Cipher audio
1	Alarm sound.wav	186/kb	0.89735	−0.00221
2	Dog barking sound.wav	279/kb	0.95292	0.00623
3	Explosion sound.wav	533/kb	0.52226	0.00161
4	Male sound.wav	345/kb	0.86710	0.00844
5	Femalesound.wav	23.3/kb	0.85605	0.00318
6	Baby sound.wav	279/kb	0.96987	−0.04283
7	Cartoon sound.wav	488/kb	0.97841	0.00154
8	Gautier sound.wav	270/kb	0.96887	0.00083
9	Lion sound.wav	221/kb	0.99856	−0.00158
10	Ref.[76]	395/kb	-	0.02021
11	Ref.[77]	-		0.00311
12	Ref.[78]	228/kb	0.815998	− 0.00938
13	Ref.[79]		−	0.00029
14	Ref.[72]		0.98153	0.000991
15	Ref.[80]	−	−	0.000852

3.5.4 Information of Entropy

The suggested encryption scheme is evaluated by information entropy. Theoretically, the ideal value of the corresponding audio scheme is 16. Consequently, a cryptosystem is considered secure if the information entropy value of the encrypted file is close to the ideal value. Table 24 summarizes the results of an information entropy analysis for the suggested cryptosystem. The suggested scheme information value is significantly closer to the ideal value for every encrypted audio data, resulting in the optimal level of uncertainty in the encrypted audio data. According to Table 24, the entropy values of various audio files ensure that the presented scheme can withstand an entropy attack, as shown in Table 24.

Table 24. Entropy analysis

S.no	Audio samples	Size/KB	Plain Audio	Cipher audio
1	Alarm sound.wav	186/kb	2.3184	4.1622
2	Dog barking sound.wav	279/kb	1.6067	4.1045
3	Explosion sound.wav	533/kb	2.6766	5.6153
4	Male sound.wav	345/kb	1.5477	4.5071
5	Femalesound.wav	23.3/kb	1.9385	4.7672
6	Baby sound.wav	279/kb	2.3182	4.1622
7	Cartoon sound.wav	488/kb	2.6223	4.7075
8	Gautier sound.wav	270/kb	2.1482	5.3487
9	Lion sound.wav	221/kb	2.3132	4.7688
10	Ref.[76]	395/kb	2.2661	5.0058
11	Ref.[77]	−	−	7.9371
12	Ref.[78]	228/kb	−	−

3.5.5 Differential analysis

An algorithm is deemed well organized and protected against differential attacks if the score of NPCR and UACI is nearly equal to 100 and 33.3333, respectively. We inspect the proposed algorithm over both analyses and observe that the suggested encryption is well-secured. The simulation score of both NPCR and UACI lies in the optimum range, as shown in Table 25. It reveals the proposed SPN structure of the encryption algorithm's significant reliance on the plan audio data and suggests that it may be more robust against differential attacks.

Table 25. Differential analysis

S.no	Audio samples	Size/KB	Npcr	UACI
1	Alarm sound.wav	186/kb	99.999721	33.341312
2	Dog barking sound.wav	279/kb	99.999823	33.442345
3	Explosion sound.wav	533/kb	99.999752	33.141256
4	Male sound.wav	345/kb	99.999602	33.341534
5	Femalesound.wav	23.3/kb	99.999501	33.445467
6	Baby sound.wav	279/kb	99.999823	33.840334
7	Cartoon sound.wav	488/kb	99.999816	33.840634
8	Gautier sound.wav	270/kb	99.999852	33.278134
9	Lion sound.wav	221/kb	99.999521	33.449134
10	Ref. [76]	395/kb	99.999506	–
11	Ref. [77]	–	99.531614	25.798423
12	Ref. [78]	228/kb	99.734812	33.687823
13	Ref. [79]	–	99.99950	33.559915
14	Ref. [72]	–	99.9997	33.3421
15	Ref. [80]	–	99.9977	–
16	Ref. [81]	–	57.23	–
17	Ref. [82]	–	99.978	32.02

3.5.6 Peak signal-to-noise ratio

We investigate the proposed algorithm by PSNR analysis to measure data quality. The peak signal-to-noise ratio (PSNR) is a decibel(dB) unite metric that quantifies the ratio between the plan and encrypted audio data, dividing by the highest power of a signal to the power of a noisy signal value. Furthermore, the high value of PSNR underscores the effectiveness of the encryption scheme. The PSNR is calculated using the following mathematical expression.

$$P_{SNR} = 20 \times log\,1\,0\left[\frac{255}{\sqrt{M_{SE}}}\right] \tag{3.17}$$

where Mean square error (MSE) is calculated via the following mathematical form

$$M_{SE} = \frac{1}{M \times N} \sum_{m}^{M} \sum_{n}^{N} [D(m,n) - E(m,n)]^2 \tag{3.18}$$

Where $D(m,n)$ Indicate the plan audio data while $E(m,n)$ is corresponding encrypted audio data. Table 26 indicates the performance analysis of PSNR and MSE of the suggested encryption algorithm. From Table 26, we can observe that the higher value of PSNR and lower value of MSE generally underscore the small amount of data retained in decrypted data. Moreover, hence the proposed algorithm is scrutinized against robustness analysis.

Table 26. Peak signal-to-noise ratio analysis

S.no	Audio samples	$Size/KB$	P_{SNR}	M_{SE}
1	Alarm sound.wav	186/kb	10.35740	3.26444×10^4
2	Dog barking sound.wav	279/kb	10.62277	3.26475×10^4
3	Explosion sound.wav	533/kb	10.22475	3.26379×10^4
4	Male sound.wav	345/kb	10.76211	3.26511×10^4
5	Femalesound.wav	23.3/kb	10.75679	3.26707×10^4
6	Baby sound.wav	279/kb	10.57626	3.26446×10^4
7	Cartoon sound.wav	488/kb	10.71392	3.26473×10^4
8	Gutier sound.wav	270/kb	10.77144	3.26493×10^4
9	Lion sound.wav	221/kb	10.56982	3.26391×10^4
10	Ref.[76]	395/kb	4.2145	–
11	Ref.[77]	–	10.7163	37.4487
12	Ref.[78]	228/kb	–	–
13	Ref.[79]	–	+4.49	–
14	Ref.[81]	–	57.30	0.1211

3.6 Asymptotic Complexity and Running Speed Analysis

This section theoretically analyzes the proposed encryption over asymptotic complexity. The asymptotic complexity summarizes the growth of the execution time with increasing input data size. It divulges the mathematical dept of the algorithm, which is independent of hardware implementation. The algorithm begins with generating random using the arithmetic operation of the elliptic curve. For this step, we used the search method for generating an elliptic curve point, which requires $O(n^2)$, operation that is the most computationally costly in the scheme. Next, the algorithm uses the random numbers and permutes the plain data, which requires $O(N \times M)$ operation, where $N \times M$ is the plain data block size. In the substitution step, the algorithm divides the permuted block data into three subblocks in constant time $O(1)$. Then substitute each subblock with a different S-box since the substitution step performs in constant time $O(1)$; therefore, for $N \times M$ block size, the step also requires $O(N \times M)$ operations. So, for $n \geq N \times M$ the whole algorithm performs $O(n^2)$ operations that are polynomial time. The running time of the entire encryption algorithm is measured in kb/second. We encrypt the different sizes of audio.wav, and the average time of encryption and decryption are 0.00334kb/sec and 0.000539 kb/sec, respectively, as shown in Table 27. Table 27 illustrates that the overall encryption steps have fewer time requirements than [76] [78]. As a result, the encryption technique is efficient and can be used for real-world communications.

Table 27. Execution time of the proposed algorithm

S.no	Audio samples	Size/KB	Encryption time/sec
1	Alarm sound.wav	186/kb	0.00221/sec
2	Dog barking sound.wav	279/kb	0.00334/sec
3	Explosion sound.wav	533/kb	1.07653/sec
4	Male sound.wav	345/kb	0.00734/sec
5	Femalesound.wav	23.3/kb	0.000539/sec
6	Baby sound.wav	279/kb	0.00334/sec
7	Cartoon sound.wav	488/kb	1.020126/sec
8	Gutier sound.wav	270/kb	0.00234/sec
9	Lion sound.wav	221/kb	0.00311/sec
10	Ref. [76]	395/kb	0.004/sec
11	Ref. [77]	–	–
12	Ref. [78]	228/kb	0.281/sec
13	Ref. [79]		0.0026/sec

3.7 National Institute of Standard and Technology (NIST) Statistical Analysis

In this subsection of security analysis, we utilize NIST statistical analysis to evaluate the Modell elliptic curve-based pseud random number sequences (MEC-PRNS) and investigate whether the suggested scheme is suitable for the cryptographic application. Since NIST tests work on binary data, convert the generated sequence to binary to ensure the randomness of the proposed algorithm. There are sixteen (16) tests in the NIST testing suite that are usually performed to examine the randomness of data, as shown in Table 28. From the table, we can notice that MEC-PRNS succeeded in the complete randomness tests of NIST, proving that the MEC-PRNS are highly random and sufficient for audio encryption.

Table 28. NIST randomness analysis for cryptographic applications

S.no	Test Name		P-Value	Result
1	Frequency-Test (single-bit)		0.93432071088934	Success
2	Frequency-Test(block)		0.31475830512155	Success
3	Run Test		0.41535210874214	Success
4	Longest Run of 1’s in a Block		0.42347212437727	Success
5	Rank test of Binary matrix		0.65746634332441	Success
6	Discrete Fourier Transform (DFT) Spectral test		0.13758358862813	Success
7	Matching Test of Non-Overlapping Template		0.21767757131905	Success
8	Matching Overlapping Template		0.16716577128047	Success
9	Maurer's Universal Statistical test (MUST)		-1.0	Not Success
10	Linear Complexity (LC) Test		0.54215767242552	Success
11	Approximate Entropy Test (AET)		0.04554663062186	Success
12	Forward Cumulative Sums (FCS) test		0.98745143218243	Success
13	Reverse Cumulative Sums (RCS) test		0.98678134070164	Success
14	Serial test (ST)		0.12491742232234	Success
15	Random Excursions Test			
	State	Chai-squared value	P −value	Result
	-4	4.123469951021149	0.5836458638476241	Success
	-3	1.744271338713358	0.8736591835003546	Success
	-2	4.844693165257315	0.4141356734512387	Success
	-1	5.240705127776518	0.4012356714687765	Success
	1	3.563295336645158	0.6475737764612386	Success
	2	4.076914662345544	0.5476836646123396	Success
	3	5.623125337746047	0.3761126757224412	Success
	4	3.5459267601847782	0.6234512475488964	Success
16	Random excursions variant test			
	State	No. of Counts	P −value	Result
	1.0	334	0.1237659854642848	Success
	2.0	353	0.2834649944849434	Success
	3.0	335	0.2347374842019319	Success
	4.0	325	0.4546373846476437	Success
	5.0	305	0.3453848434811987	Success
	6.0	298	0.3645367465353636	Success
	-1.0	251	0.4763544688436878	Success
	-2.0	248	0.1234687473534484	Success
	-3.0	253	0.7464364454193768	Success
	-4.0	276	0.1236294849734841	Success
	-5.0	247	0.5378486462354648	Success
	-6.0	253	0.6473543878434384	Success

Chapter 4

Hyper Elliptic Curve for Efficient Digital Image Watermarking

The availability of multimedia data across the world wide web has affected unintended individuals in distributing information, including images, audio, and videos, information illegally. Problems with copyright protection and ownership authentication are highly prevalent, so to counter these issues, it is also required to strengthen the secured strategy. The unauthorized distribution of multimedia data is shown in Figure 20. As a result, an authorized, highly secured strategy is required to identify these unlawful users to end illegal data distribution. In addition, digital watermarking provides anti-tampering, access control, ownership verification, non-repudiation, indexing, memory savings, and requirements of bandwidth limitations. There are some fundamental principles to applying Watermarks digitally in the images: (1) Maintaining the quality of the host's image is essential; (2) inside the host image with a watermark, and the watermark is kept hidden; (3) keeping it protected from unauthorized users, the watermark should be irregular and invisible. Moreover, the classification of digital watermarking according to their domain is shown in Figure 21 [83], [84].

In [85], hybrid multiple watermarking(HMW) is present in the transform domain. In the proposed work, the author used the combination of discrete wavelet transformation (DWT), singular value decomposition (SVD) and discrete cosine transformation (DCT) instead of individuals domain to improve the robustness and quality of the watermark image. However, it's possible that it somewhat increased computational complexity, which has to be looked into independently. A reversible watermarking approach is developed in [86], for healthcare applications. The suggested approach utilized the technique of pixel-to-block (PTB) for the generation of a cover image instead of the conventional procedure.

Considering the above-mentioned copyright protection and ownership authentication problems, this chapter proposed an efficient digital watermarking based on the hyperelliptic curve, which is the generalisation of an elliptic curve. The suggested technique is key-dependent, and only the main owner of the image may authenticate his ownership using his secret key. The suggested approach utilizes random sequences generated using the HEC and distributes the watermark image data randomly. On the one hand, the random distribution of the watermark image does not influence the quality of the host image; on the other hand, this technique strengthens the security of the proposed system since only the authorised owner may replicate the watermark image. Furthermore, the chapter is concluded with the analytical findings of the suggested system and its comparison with the existing excellent literature.

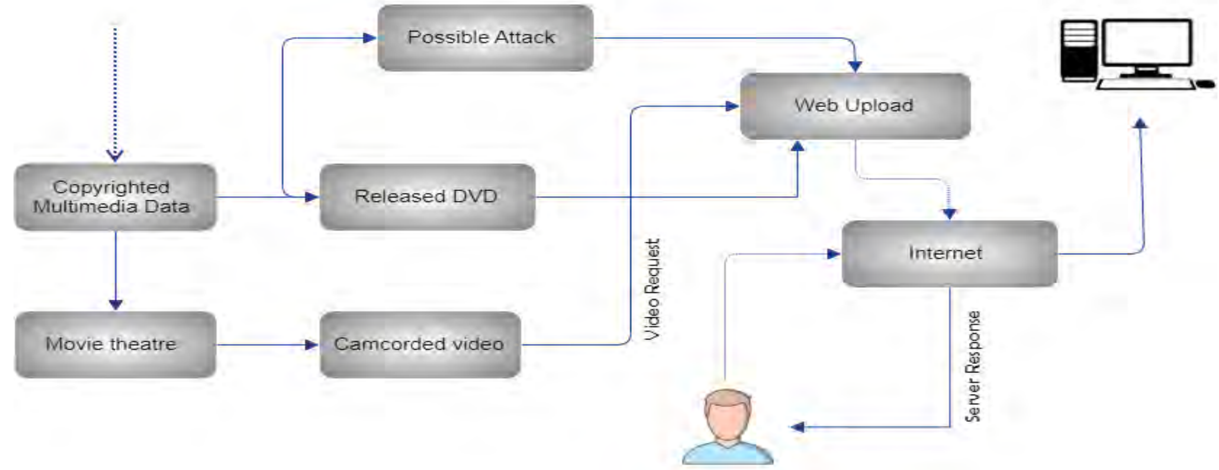


Figure 20. Unauthorized distribution of video data

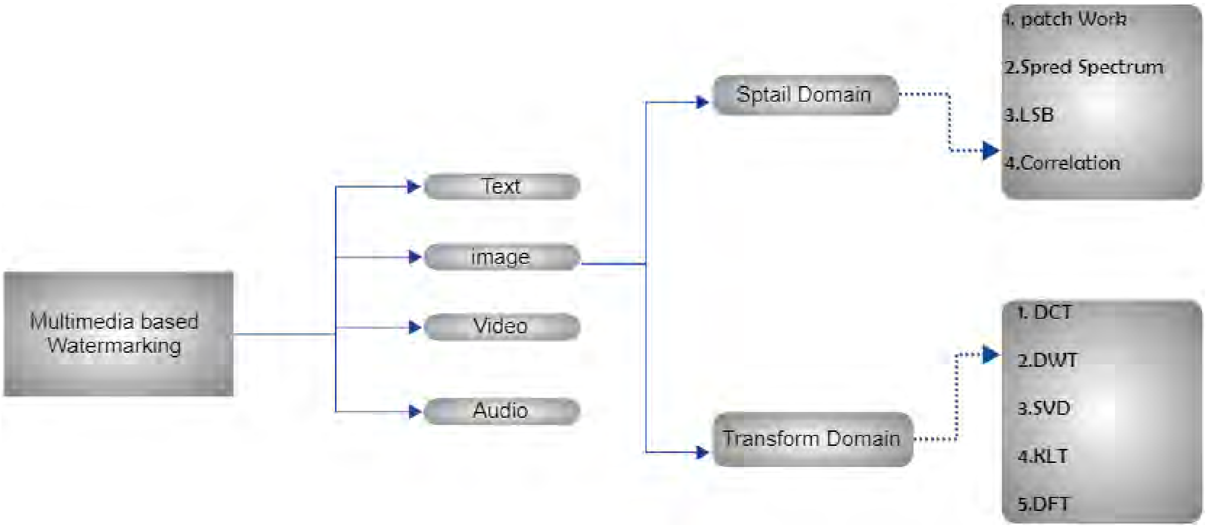


Figure 21. Watermarking embedding techniques with Domain-specific categorization

4.1 Fundamentals of Hyper Elliptic Curve

As part of this section, we looked at a few basic definitions of HEC over a finite field and their characteristics employed in the proposed watermarking technique. A hyperelliptic curve $\mathcal{C}$ of genus $\mathcal{G}(\mathcal{G} \geq 1)$ defined over the finite field $\mathcal{K} = \mathcal{F}_q$ as defined as[87]:

$$\mathcal{C} = \mathcal{Y}^2 + \mathcal{H}(\mathcal{X})\mathcal{Y} = \mathcal{F}(\mathcal{X}) \ in \ \mathcal{K}[\mathcal{X}, \mathcal{Y}] \tag{4.1}$$

Where $\mathcal{H}(\mathcal{X})$ and $\mathcal{F}(\mathcal{X}) \in \mathcal{K}[\mathcal{X},\mathcal{Y}]$ is a polynomial of degree at most $\mathcal{G}$ and $2\mathcal{G}+1$ respectively, and there are no such points $(\mathcal{X},\mathcal{Y})$ on closer filed $\bar{\mathcal{K}} \times \bar{\mathcal{K}}$, which satisfies the following equations.

$$\mathcal{Y}^2 + \mathcal{H}(\mathcal{X})\mathcal{Y} = \mathcal{F}(\mathcal{X}) \tag{4.2}$$

$$2\mathcal{Y} + \mathcal{H}(\mathcal{X}) = 0 \tag{4.3}$$

$$\mathcal{H}(\acute{\mathcal{X}}) - \acute{\mathcal{F}}(x) = 0 \tag{4.4}$$

The point $(\mathcal{X},\mathcal{Y}) \in \bar{\mathcal{K}} \times \bar{\mathcal{K}}$ which satisfies the equations from eq.(4.2-4.4) is called a singular point. A hyperelliptic curve has no singular point.

4.1.1 Opposite and Special Point

Consider the $p_{hec} = (x, y)$ be the HEC point, then the opposite point of $\tilde{p}_{hec} = (x, -\mathcal{Y} - \mathcal{H}(x))$, while the special point on HEC is 0 called the point of infinity.

4.1.2 Arithmetic of Hyper Elliptic Curve

The points on an elliptic curve with a point of infinity $\{\infty\}$ can be grouped to form a group. However, for hyperelliptic curves, taking the points on the curve $\mathcal{C}$ and adding the points of infinity, we will not be able to form a group. To form a group of points in the hyperelliptic curve, we must take the sum of the points as group elements and then add them as follows:

$$(\mathcal{P}_1 + \mathcal{P}_2) \oplus (\mathcal{Q}_1 + \mathcal{Q}_2) = (\mathcal{R}_1 + \mathcal{R}_2) \tag{4.5}$$

While symbols $+$ and $\oplus$ do not represent addition and XOR operations, respectively, the xor operation represents the mathematical operation of the group.

4.1.3 Divisor

In cryptography, the hyperelliptic curve computes groups that are subgroups of the random group $\mathcal{D}$ resulting from the set of points on the curve. If the curve $\mathcal{C}$ is the HEC of genus $\mathcal{G}$ over the finite field $\mathcal{F}_q$. The elements of $\mathcal{D}$ are known as divisors. The divisor $\mathcal{D}$ is defined by the following mathematical expression [87] .

$$\mathcal{D} = \sum m_{\wp}\mathcal{P} \qquad m_{\wp} \in \mathcal{F}_q\, , \mathcal{P} \in \mathcal{C} \tag{4.6}$$

Where is $\mathcal{D}$ is the reduced divisor and $m_{\wp}, \mathcal{P}$ are the number of points and points on the curve $\mathcal{C}$.

4.1.4 Group Divisors

The group divisors ${div_c}^0$ of hyperelliptic curve $\mathcal{C}$of genius $\mathcal{G}$ and degree 0 are Computed by the following mathematical formula.

$div_c{}^0 = \sum_{\mathcal{P}\in\mathcal{C}} m_{\wp}\mathcal{P} \,|m_{\wp} \in \mathcal{F}_q, m_{\wp} = 0$ for most of the points on the curve $\mathcal{P} \in \mathcal{C}$ (4.7)

4.1.5 Divisor class group

Each divisor class in the divisor class group can be represented as:

$$\mathbb{D} = \sum_{i=1}^{r} \mathcal{P}_i - r\mathcal{P}_\infty , \mathcal{P}_i \in \mathcal{C} \cup \mathcal{P}_\infty,\ r \leq \mathcal{G} \tag{4.8}$$

4.1.6 Jacobian of Hyper Elliptic Curve

The Jacobian of the curve $\mathcal{C}$ defined over the finite field $\mathcal{F}_q$ is denoted by $\mathcal{J}_c(\mathcal{F}_q)$. The mathematical formulation of the Jacobian of the curve $\mathcal{C}$ is defined as:

$$\mathcal{J}_c(\mathcal{F}_q) = {}^{div_c{}^0}/_{\mathcal{P}} \tag{4.9}$$

Where every element of the $\mathcal{J}_c(\mathcal{F}_q)$, can be represented uniquely by divisors $\mathcal{D}$. Hence if $\mathcal{D}_1, \mathcal{D}_1 \in div_c{}^0$ are equivalent if $\mathcal{D}_1 - \mathcal{D}_1 \in \mathcal{P}$. There is precisely one divisor in every equivalence class called the reduced divisor. The group law is formed by the reduced divisor, represented by Mumford representation [88].

4.1.7 Mumford Representation

Mumford representation is the simplest representation of the Cartesian points in polynomial divisor form. The divisor can be represented by a pair of polynomials as $u(x), v(x)$. Although both polynomials, i.e., $u(x), v(x) \in \mathcal{F}_q$, and must satisfy the following condition.

$$u(x) \text{ is monic polynomial} \tag{4.10}$$

$$\deg\,(v(x)) < \deg\,(\,u(x)\,) \leq \mathcal{G} \tag{4.11}$$

$$u(x)|v(x)^2 + v(x)\,\mathcal{H}(\mathcal{X}) - \mathcal{F}(\mathcal{X}) \tag{4.12}$$

The divisor class polynomial $u(x)$ is represented by the following mathematical equation.

$$u(x) = \prod_{i=1}^{r} x - x_i \tag{4.13}$$

Where the divisor class $\mathbb{D}$ is shown in equation (4.8).

4.1.8 Cantor's Algorithm

In the jacobine of a hyperelliptic curve, i.e., $\mathcal{J}_c(\mathcal{F}_q)$The cantor's algorithm presents the formula for executing arithmetic group operations such as divisor addition and doubling [88]. The cantor's algorithm on the divisor is performed in a two-step. (1). Determined the reduced divisor $\mathcal{D}' = div(u', v')$ such that $\mathcal{D} = \mathcal{D}_1 + \mathcal{D}_2 = div(u_1, v_1) + div(u_2, v_2)$ in the group of jacobine $\mathcal{J}_c(\mathcal{F}_q)$. (2). Find the semi-reduced divisor $\mathcal{D}' = div(u', v')$ to an equivalent $\mathcal{D} = div(u, v)$. Table 29 briefly explains the algorithm for the divisors' adding and doubling [89].

Table 29. Algorithm for Adding and Doubling the divisors

Algorithm for Adding two divisors

```
**Input:** $\mathcal{D}_1 = div\left(u_{1_p}, v_{1_p}\right)$, $\mathcal{D}_2 = div\left(u_{2_q}, v_{2_q}\right)$, $\mathcal{C} = \mathcal{Y}^2 + \mathcal{H}(\mathcal{X})\mathcal{Y} = \mathcal{F}(\mathcal{X})$.
**Output:** $\mathcal{D}_3 = \mathcal{D}_1 + \mathcal{D}_2 = div\left(u_{3_r}, v_{3_r}\right)$.
*Step 1: Compute the gcd using the Extended Euclidean Algorithm(EEA).*
$\mathbb{D} = gcd(u_{1_p}, u_{2_q}, v_{1_p} + v_{1_p} + \mathcal{H}) = a_1 u_{1_p} + a_2 u_{2_q} + a_3(v_{1_p} + v_{1_p} + \mathcal{H})$.
*Step 2: Calculate $U'$ Using the below expression.*
 $U' = u_{1_p} u_{2_q} \mathbb{D}^{-1}$.
*Step 3: Calculate*
$\left[a_1 u_{1_p} u_{2_q} + a_2 u_{2_q} u_{1_p} + a_3\left(v_{1_p} v_{2_q} + \mathcal{F}\right)\mathbb{D}^{-1}\right] mod\ U'$ .
**Step 4:** Initialize $j = 0$
 $While$ deg ( $U'_j$) $> \mathcal{G}$ do
   $j = j + 1$;
   $U'_j = \dfrac{\mathcal{F} - v'_{j-1}\,\mathcal{H}(v'_{j-1}{}^2)}{U'_{j-1}}$
   $v'_j = \left(-\mathcal{H} - v'_{j-1}\right) mod\ U'_j$
     $end$
 **Output:**  $(u_{3_r}, v_{3_r}) = (U'_j, v'_j)$.
```

Algorithm for divisors doubling

```
*Step 1:* $\mathbb{D} = gcd(U, 2V + \mathcal{H}) = a_1 U + a_3(2v + \mathcal{H})$
*Step 2:* $U' = (U^2\ \mathbb{D}^{-2})$
*Step 3:* $V' = [a_1 UV + a_3(V^2 \mathcal{F})\mathbb{D}^{-1}]\ mod\ U'$.
```

4.2 Proposed Colour Image Watermarking Technique

In this section, we prosed a new digital colour image watermarking technique based on the mathematical operation of HEC. Initially, the uniform permutation process uses hyperelliptic curve pseudo-random number generation (HEC-PRNG); the brief watermarking image description is given in subsection 4.3.1. After that, the embedding and extraction of the host image using the most significant bit(MSB) and the least significant bit(LSB) and their inverse process are given in subsections 4.3.3 and 4.3.4.

4.2.1 Proposed Watermarking Image Technique

The suggested colour watermark image technique works in the following steps.

Step 1: Load the Host image H of size $m \times n \times 3$.

Step 2: Generate the points on HEC $\mathcal{C} = \mathcal{Y}^2 + \mathcal{H}(\mathcal{X})\mathcal{Y} = \mathcal{F}(\mathcal{X})\ in\ \mathcal{K}[\mathcal{X}, \mathcal{Y}]$ of $\mathcal{G}$ =2, Where $\mathcal{F}(\mathcal{X})$, be defined as in eq (14) with the condition in eq(2-4) must be satisfied.

$$\mathcal{F}(\mathcal{X}) = x^5 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \qquad (4.14)$$

Step 3: Next, the generated points on HEC are permuted to their opposite point. The mathematical formulation of the HEC point to their opposite point is given in equation (4.15).

$$hec: \mathcal{F}_q \times \mathcal{F}_q \rightarrow \mathcal{F}_q \times \mathcal{F}_q$$

$$hec(x_i, y_j) = (x_{i'}, y_{j'})$$
$$(x_{i'}, y_{j'}) = (x_i, -y_j - \mathcal{H}(x))$$
$$hec(x_{i'}, y_{j'}) = y_{j'} \tag{4.15}$$

While $(x_{i'}, y_{j'})$ are opposite points of HEC. After that, pick the coordinate $y_{j'}$, of any dimension and perform the row and column-wise cyclic permutation(RCWCP) on the host image. The detailed procedure of RCWCP is given in subsection 4.3.2

Step 4: Load the watermark-Logo image H', of dimension $u \times v \times 3$ and convert the watermark image H' Into MSB and LSB, then MSB converts to LSB.

Step 5: Dived the permuted host image of dimension $\mathcal{m} \times \mathcal{n} \times 3$ into the subblock of dimension $u \times v \times 3$.

Step 6: Embedded the LSB of the watermark-Logo image into the MSB of the sub-block of the permuted host image of dimension $u \times v \times 3$. The detailed procedure for the embedding and extracting process is given in subsections 4.3.3 and 4.3.4

Step 7: Execute the row and column-wise cyclic permutation in reverse order to get the watermarked image $\mathbb{W}$.

Step 8: To extract the watermark logo from the watermarked image, perform the steps in reverse order to get the extracted watermark-Logo.

4.2.2 Row and Column Wise Cyclic Shift Permutation

The pixels in a host image H are listed in $\mathcal{m}$ rows and $\mathcal{n}$ columns. For the row-wise permutation(RWCP), the term $y_1 \in y_{j'}$ was chosen from a sequence generated by HEC to permute the pixels by the row-wise cyclic shift operation. For each row, a new random term was chosen from $y_{j'}$ to permute every row by RWCP of the watermark image. However, there are no restrictions on the initial term y_1; choose any term from the sequence and iterate the process on the watermark image of $\mathcal{m}$ rows. For example, $y_1 \in y_{j'} = [2,1,2,1 \ldots, \ldots, \mathcal{m}]$, and let H be an image of $\mathcal{m}$ rows, the first row pixels $\mathcal{R}_{1C} \in H$ permute first-row cyclic shift to the right or left direction by 2. Moreover, receivers should perform cyclic shift operations right to left if senders perform them left to right. Otherwise, the receiver should not get a plan image permuted by the sender row-wise. The mathematical construction is given below in eq (4.16).

$$y_{j'} = [2\ 1\ \ldots, \ldots, \mathcal{m}]$$

$$\begin{bmatrix} \mathcal{R}_{1C_1} & \dots & \cdots & \mathcal{R}_{1C_n} \\ \mathcal{R}_{2C_1} & \dots & \dots & \mathcal{R}_{2C_n} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \mathcal{R}_{mC_1} & \dots & \dots & \mathcal{R}_{mC_n} \end{bmatrix} \rightarrow \begin{bmatrix} \mathcal{R}_{1C_{n-1}}\ \mathcal{R}_{1C_n} & \dots & \cdots & \mathcal{R}_{1C_{n-2}} \\ \mathcal{R}_{1C_{n-1}}\ \mathcal{R}_{2C_1} & \dots & \dots & \mathcal{R}_{2C_{n-1}} \\ \dots, \dots\dots & \dots & \dots & \dots \\ \dots, \dots\dots & \dots & \dots & \dots \\ \mathcal{R}_{mC_1}, \dots\dots. & \dots & \dots & \mathcal{R}_{mC_n} \end{bmatrix} \tag{4.16}$$

Like the RWCP, the column-wise cyclic permutation (CWCP) is executed by n columns by choosing any random element from $y_{j'}$, and permuting the pixels of a column by cyclic shift operation from right to left or left to right direction. For example, $y_1 \in y_{j'} = [2,1,2,1 \dots, \dots, n]$, and let H be an image of n columns. Choose the first column $C_{1R} \in H$ and execute the cyclic shift operation on the row by 2 from the left /right direction. The first-row cyclic shift to the right or left direction by 2. Furthermore, cyclic shift operations should be performed right to the left by receivers if they are performed left to right by senders. Otherwise, the receiver should not receive a plan image that the sender has permuted cyclic shift operation column-wise. The mathematical description of CWCP is given below in eq (4.17).

$$y_{j'} = [2\ 1\ \dots, \dots, m]$$

$$\begin{bmatrix} C_{1r_1} & \dots & \cdots & C_{nr_1} \\ C_{1r_2} & \dots & \dots & C_{nr_2} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ C_{1r_m} & \dots & \dots & C_{nr_m} \end{bmatrix} \rightarrow \begin{bmatrix} C_{1r_{m-1}}\ C_{2r_m} & \dots & \cdots & \mathcal{R}_{1C_{k-2}} \\ C_{1r_m}\ \ C_{2r_1} & \dots & \dots & \mathcal{R}_{2C_{k-1}} \\ \dots, \dots\dots & \dots & \dots & \dots \\ \dots, \dots\dots & \dots & \dots & \dots \\ C_{1r_{m-2}}, C_{2r_{m-1}}. & \dots & \dots & \mathcal{R}_{mC_k} \end{bmatrix} \tag{4.17}$$

4.2.3 Watermarking Embadding

The processes for embedding a watermark image are as follows, given a watermark image H of size $m \times n \times 3$ and the host image H' , of dimension $u \times v \times 3$. Initially, the watermark image H is permuted into H_1 using HEC-PRNG to vanish the adjacent pixel correlation, and the data is uniformly distributed. Next, dived the watermark permuted H_1 image into the non-overlapping $u_i/128 \times v_i/128$ sub-blocks of dimension $u \times v \times 3$. After that, $u_1/128 \times v_1/128$ of dimension $u \times v \times 3$ say H_2 and the host image converts to the MSB of all three layers, namely $H^R{}_2, H^G{}_2, H^B{}_2$ H'^R, H'^G, H'^B, respectively, then convert the MSB of the host image into LSB and add them with the corresponding layer of each image to embed the watermark. The mathematical expression for the embedding procedure is given below.

$$MSB(H_2) = msb(H^R{}_2)$$

$$= msb({H^G}_2)$$

$$= msb({H^B}_2). \tag{4.18}$$

$$LSB(H') = lsb(msb({H'}^R)$$

$$= lsb(msb({H'}^G),$$

$$= lsb(msb({H'}^B). \tag{4.19}$$

$$EMbadding = MSB(H_2) + LSB(H'). \tag{4.20}$$

4.2.4 Watermarking Extraction

The extraction process of watermarked image is relatively the same as the watermarked embedding. Consider the watermarked image 𝕎 and the symmetric key generated by HEC are received. The following steps involved in watermarked extraction are as follows.

Initially, load the watermarked image 𝕎 and permute RWCP as a key to extract the permuted image. Next, divide this permuted image into subblocks $u_i/128 \times v_i/128$ $\mathcal{A}$ of dimension $u \times v \times 3$. Then, extract the MSB from $\mathcal{A}$ and convert it to LSB; the LSB convert to MSB and subtracted from the subblock to get the extracted MSB watermark-logo H'. The following mathematical expressions compute the extraction of the watermark logo.

$$\mathcal{A}_1^r = msb(lsb(msb(\mathcal{A}^r\ ))$$
$$\mathcal{A}_1^g = msb(lsb(msb(\mathcal{A}^g\ ))$$
$$\mathcal{A}_1^b = msb(lsb(msb(\mathcal{A}^b))$$
$$H^{r\prime} = msb(\mathcal{A}^r - \mathcal{A}_1^r)$$
$$H^{g\prime} = msb(\mathcal{A}^g - \mathcal{A}_1^g)$$
$$H^{b\prime} = msb(\mathcal{A}^b - \mathcal{A}_1^b)$$
$$H' = concatenate(H^{r'}, H^{g'}, H^{b'}). \tag{4.21}$$

Where, $H^{r\prime}$, $H^{g\prime}$, $H^{b\prime}$, the extracted MSB of the watermark logo. The flow chart of the proposed watermarking technique is shown in Figure 22.

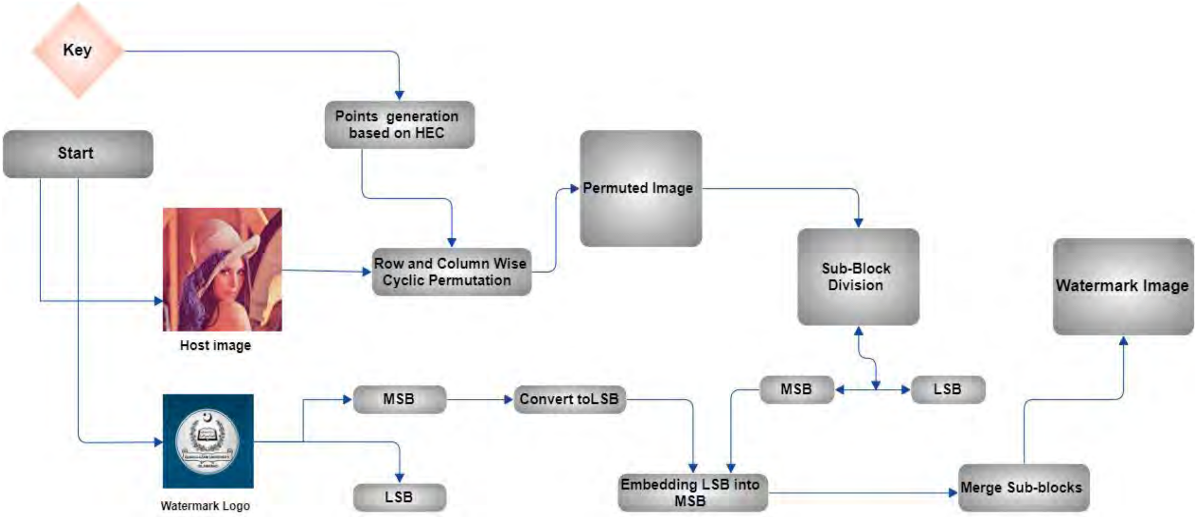


Figure 22. Flow Chart of The Proposed Watermarking Technique

4.3 Evaluation Metrics and Simulation Results of the Proposed Technique

To examine the suggested scheme, the watermarking approach is simulated by Matlab R2021a. The colour images of pepper, baboon, and Lena, of dimension 512×512 and the watermark colour image Qau monogram of dimension 128×128, data set used in the section of experimental analysis.

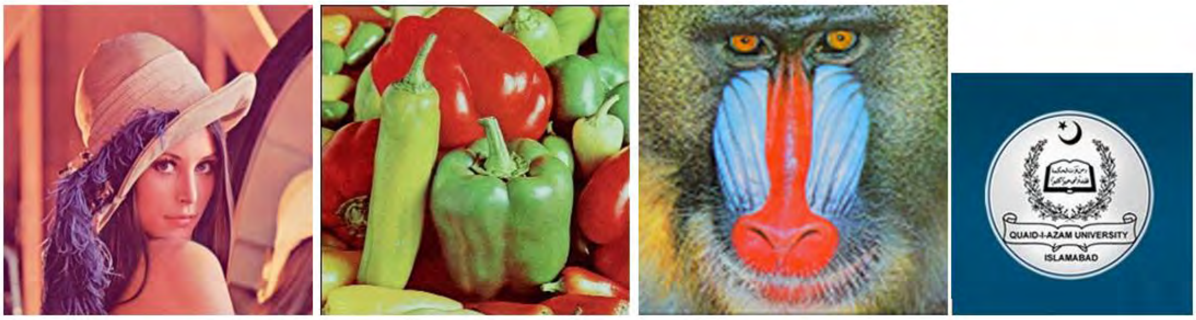


Figure 23. Data Set used in the Proposed algorithm

4.3.1 Quality and Effectiveness Metrics

The proposed digital colour watermarking technique is evaluated by the effectiveness and the quality, such as mean square error (MSE), peak-to-signal noise ratio(PSNR), and structurally similarity index(SSIM), which we have already explained in chapter 2.

4.3.2 Structural Similarity Index

The proposed watermarking scheme is evaluated by the structural similarity index(SSIM) to examine the quality of the original and recovered image difference. The obtained value of SSIM of the proposed watermarking scheme is nearly close to 1. The calculated difference between the original and recovered watermark image is 1, indicating that the watermark has not been altered in the public channel.

4.3.3 Mean Squared Error

It evaluates the quality of the image and validates the average squared difference between the original and recovered host image [90][91][92][93][94]. The mathematical representation of MSE is defined as:

$$\mathcal{MSC} = \sum_{i=0}^{N-1}\sum_{j=0}^{M-1} \frac{[O(i,j) - |R(i,j)|]^2}{M \times N} \tag{4.22}$$

Where $O(i,j)$, and $R(i,j)$ represent the original and recovered host image of dimension $M \times N$. We examined our proposed watermarking technique by $\mathcal{MSC}$ analysis for the baboon and peepers images of dimension 512×512. The computed value of $\mathcal{MSC}$ of baboon and peepers images is 0, which is very low. Similarly, the numerical value of MSE of the original images of baboon and peppers and their watermark comes to 0.0000745, which is very low. Furthermore, the MSE value of the watermark and the extracted watermark is less, ensuring that the proposed algorithm shows the robustness of the watermark.

4.3.4 Peak Signal-to-Noise Ratio

We examined the proposed algorithm by the peak signal-to-noise ratio(PSNR). The theoretical and mathematical description of PSNR matrices is given in chapter 2. The PSNR value of the original host and the recovered image is 97.24430, which ensures that the proposed algorithm show robustness against PSNR analysis.

4.4 Experimental Analysis of Watermark Image

Watermark image is unprotected from various kinds of attacks. These attacks are categorised into Geometric or Transform, Noising, Roubstaness and Counterfeiting attacks. In a geometric attack, the attacker can modify the geometry of the image by altering its rotation, scale, or translation. In the category of the robustness of the watermark, the attacker usually removes the watermark logo through JPEG compression and image cropping. In a noise watermark attack, add some different types of noise to the watermark. In a Counterfeiting attack, the active attacker captures the original image, and instead of it, the attacker forwards the fake/forged image.

4.4.1 Salt and Pepper Attack

Salt and Pepper attacks were calculated based on their impact on recovered image quality [95]. We added salt and pepper noise with different ratios of the proposed algorithms and extracted the watermark. From the salt and pepper noise attacks, we observe that, with the increase of noise in the watermark image, the PSNR value decrease and vice versa, as shown in Table 30.

The illustration of a baboon, Lena, and pepper of watermark image of dimension 512×512 with salt and pepper noise is shown in Figure 24, with extracted watermark Qau monogram.

4.4.2 Rotation Attack

We perform the rotation attacks on the watermark images of the baboon, Lena, and pepper. There are two approaches to fulfilling the rotation attacks; the first one rotates both the original and watermark image by $10^{\circ}, 15^{\circ}, 30^{\circ}$ and the second one rotates the watermark image by $10^{\circ}, 15^{\circ}, 30^{\circ}$ Clockwise and then anti-clockwise. The SSIM value of the watermarked image varies from 1 to 0.341320 for the rotation attack 10°. The illustration of the rotation attack of the baboon, Lena and pepper using the second approach is shown in figure 25. We observe from the rotation attack that the proposed watermarking techniques are robust against rotation attacks

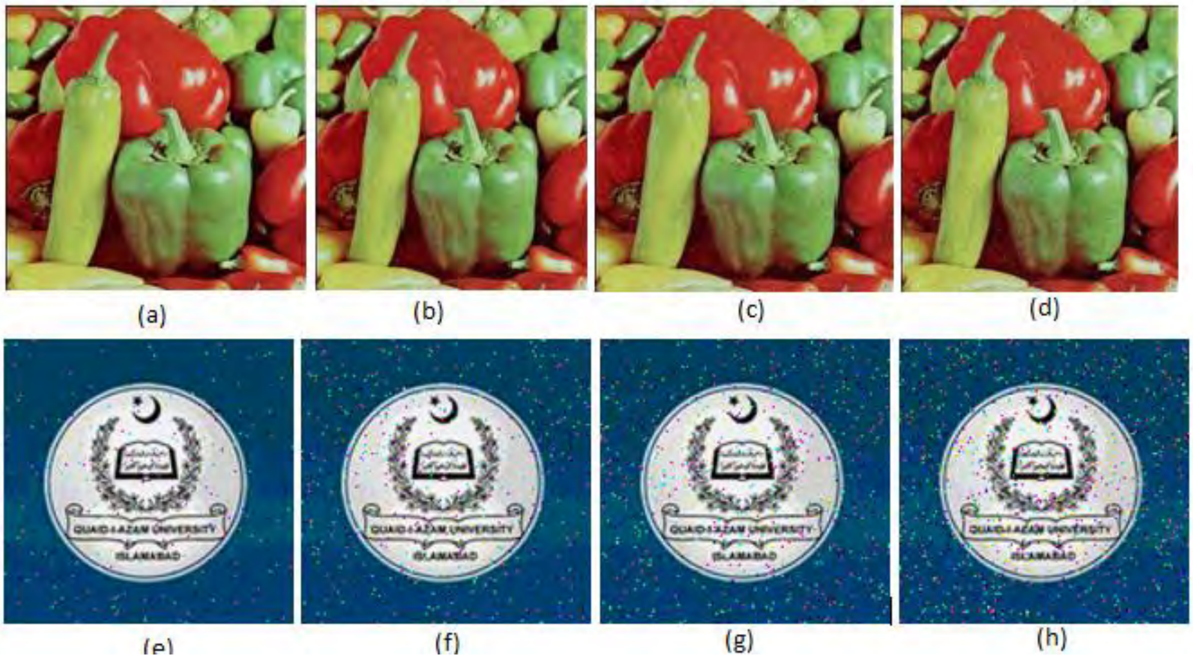


Figure 24. (a-d)Salt and Pepper Noise with different ratios (e-h)Crossponding their extracted watermark logo.

Table 30. Salt and peppers analysis on watermark image

Attacks ratio	PSNR values			Observation
Images	Pepper	Lena	Baboon	From the PNSR results, we observe that without the salt and pepper noise, the value of PSNR increased, while when the ratio Noise increased, the PSNR value decreased.
Without Noise	24.5137	24.6138	24.6147	
0.1 Noise	21.2345	21.7745	21.7325	
0.2 Noise	16.4675	16.2375	16.6685	
0.3 Noise	15.2536	15.6536	15.4536	
0.4 Noise	14.2345	14.4245	14.7464	

.

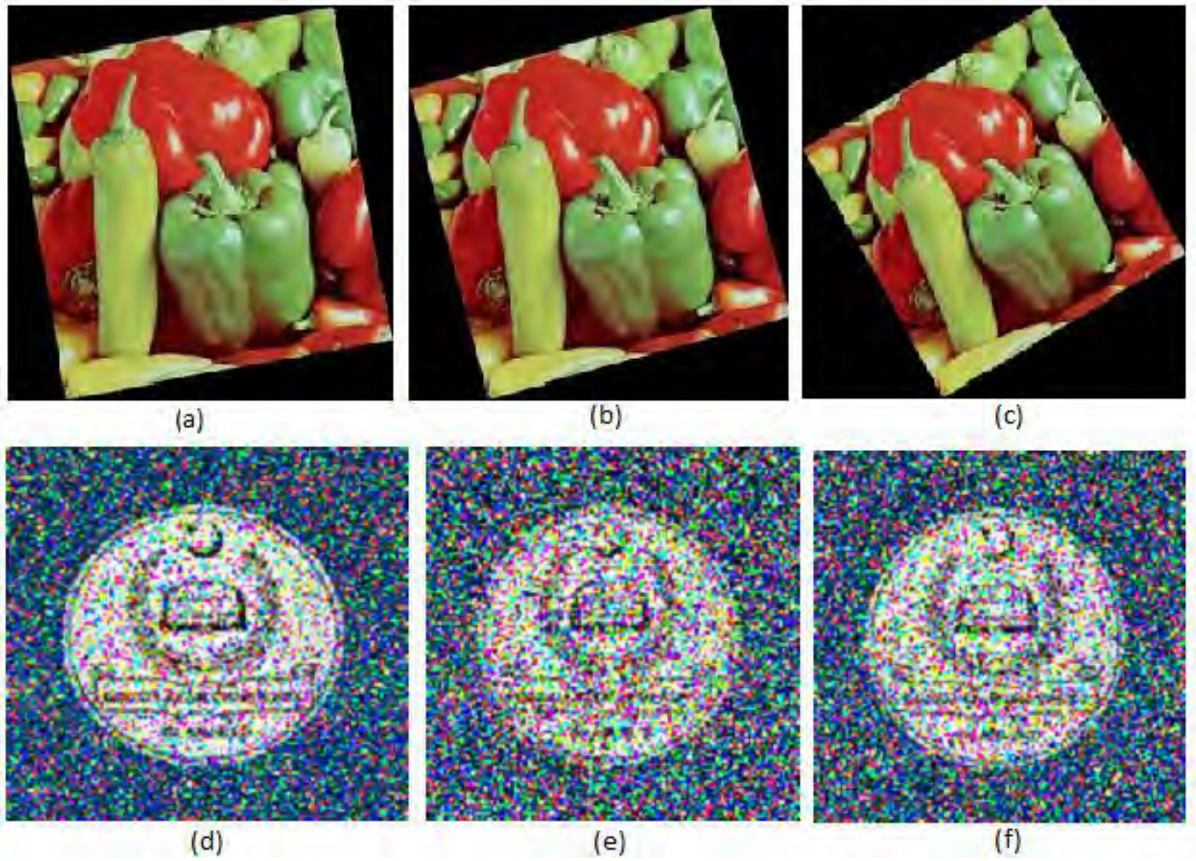


Figure 25. (a-c) Rotation attacks with different angles(d-f) Crossponding extracted watermark logo

4.4.3 Cropping Attack

We evaluate the proposed watermarking approach by cropping attacks. We crop the watermark image peppers by 25% from the upper left and right, 25% from the bottom left and right, and then extract the watermark logo. The difference in SSIM between the cropped image and the original host watermarked image is 0.21346. The illustration of cropping attacks is shown in Figure 26. Figure 26 shows that the suggested watermarking scheme is robust against cropping attacks.

4.4.4 Compression Attack

When a watermarked image isn't already in JPEG format, the attacker can easily convert it into one by reducing the quality factor of JPEG compression until the image loses the characteristics he wants [95]. Moreover, it is possible for the attacker to resave the watermarked image as a JPEG, even if it is already a JPEG with a lower quality factor. Due to the standard and easy nature of JPEG attacks, this robustness assessment emphasises a robust response to JPEG compression. We implement the compression attack on the watermark image. The image is compressed to the size of $(256 * 256)$. Moreover, the difference in SSIM value between the cropped image and the original host watermarked image is 0.89346, which ensures that the watermark image has been attacked in a public channel. The illustration of JPEG compression attacks of Lena, the baboon, and pepper watermarked image is shown in Figure 27. Figure 27 ensures that the proposed watermarking technique is robust against compression attacks.

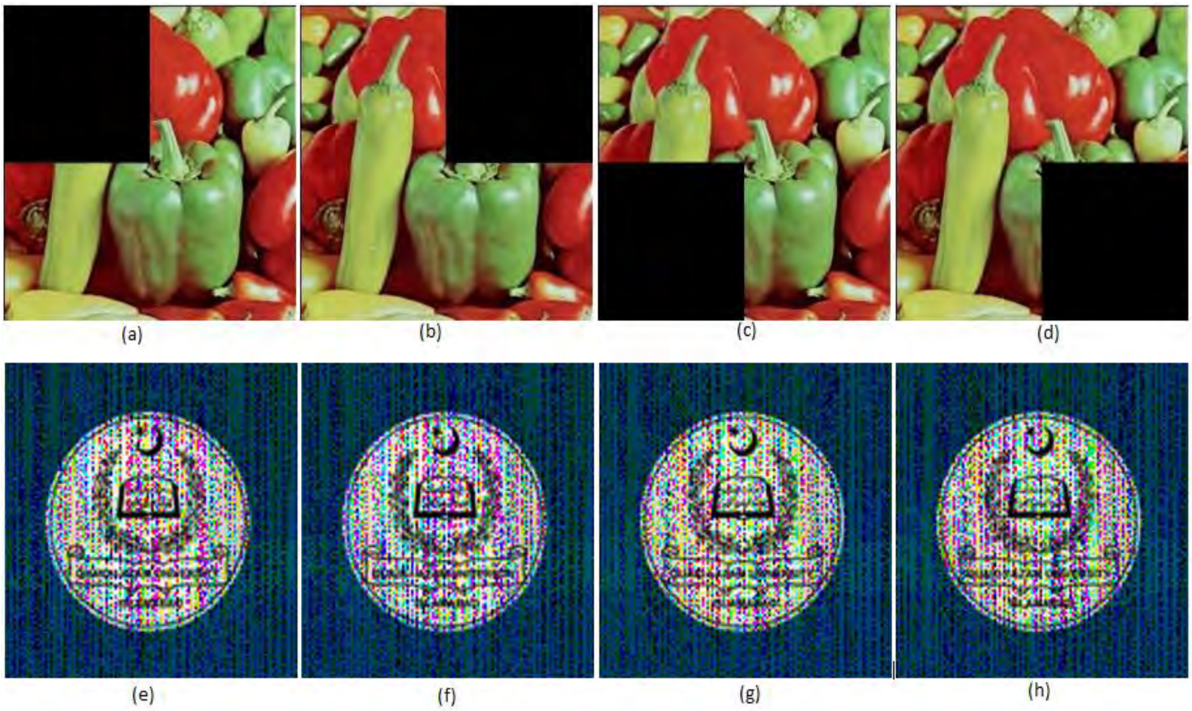


Figure 26. (a-d) Cropping Attacks of the original image Peppers with different data lose (e-h) corresponding extracted watermark logo

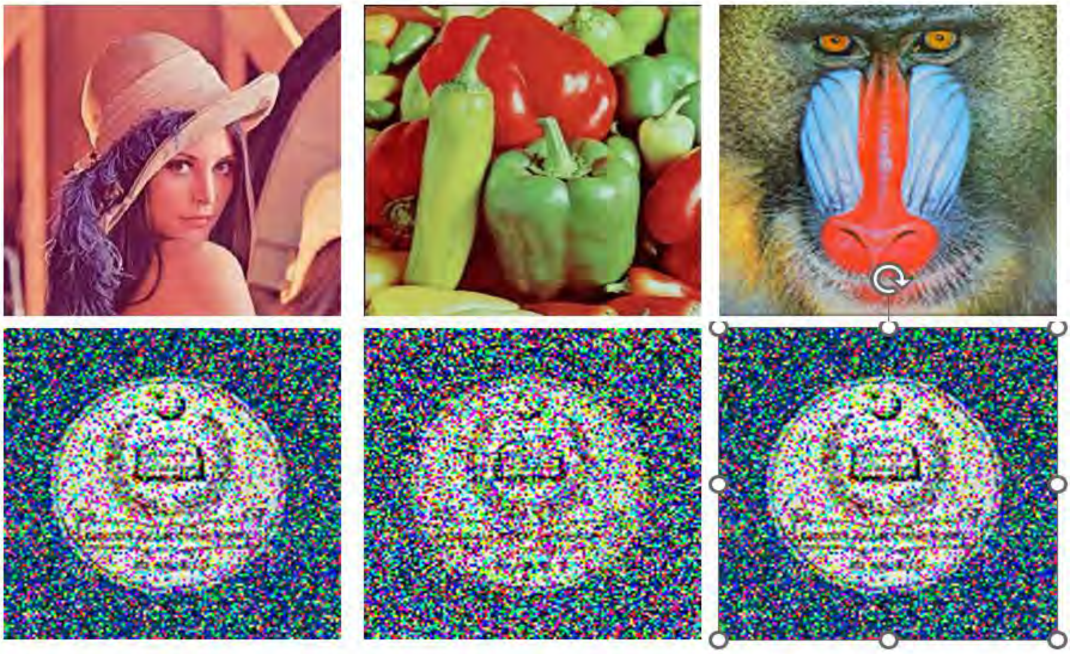


Figure 27. First row shows the Compression attacks of the original image Lena, Peppers and Baboon of Dimension $256 * 256$. The second row shows the corresponding extracted watermark logo

Table 31. Analysis of the original host and watermark image

	SSIM	CC	Observation
Pepper	0.89346	0.001359	The SSIM value is entirely different between the original and encrypted images. The value of CC is less to ensure the difficulty level for the attacker
Lena	0.097554	0.0065466	
Baboon	0.15467	0.006356	

Table 32. Experimental analysis of original and recovered image

	SSIM	PSNR	MSE	Observation
Pepper	0.956721	97.24430	0.000002	The value of MSE is significantly less. The value of PSNR for both images is very high. The SSIM value is close to 1.
Lena	0.97644	88.35657	0.0000004	
Baboon	0.98446	91.46575	0.0000003	

4.5 Comparison with other Existing Algorithms

We compared the proposed digital watermarking scheme with other algorithms in this subsection. The proposed watermarking robustness is evaluated through the stat of art metrics like PSNR, SSIM, MSE and CC. the proposed algorithm has a high PSNR value of 97.24430, indicating a high-quality level and robustness compared to other existing watermarking algorithms [95]–[100]. Moreover, the value of SSIM of the suggested scheme is close to 1, which ensures that the proposed cryptosystems show high robustness of the watermark image as compared to the existing watermark techniques [95]–[100]. Additionally, time embedding is an essential factor in evaluating the effectiveness of the watermark algorithm. We compare the proposed scheme by an important factor of time embedding. According to the findings shown in Table 33, our suggested strategy outperforms several current methods [95]–[100] in terms of embedding time.

Table 33.Comparative Analysis

	SSIM	PSNR	MSE	CC	Emmbiding time
Proposed	0.956721	97.24430	0.000002	0.001359	0.8754/sec
Ref.[95]	0.999935	97.5450	0.0000001	0.002287	No
Ref.[96]	0.9150	55.6042	N0	0.8375 (NC)	N0
Ref.[97]	0.9992	56.8684	N0	0.9998(NC)	4.337/sec
Ref.[98]	0.99993	52.5768	No	0.99999(NC)	251.79/sec
Ref. [99]	No	38.64	No	No	1.275/sec
Ref.[100]	0.9771	37.7256	N0	1	8.062/sec

Chapter 5

Gray Scale Image Encryption based on Isomorphic Elliptic Curves

Multimedia data is an essential source for delivering information over the network and is widely used in many fields. The most important one is the digital image, which has significant information panache and is often used to exchange digital information. However, due to open network development, the secrecy of those images which contain sensitive information during transmission is the central issue. Advanced Encryption Standard (AES), Data Encryption Standard (DES) [101], and triple data encryption standard (TDES) [102] are efficient cryptographic algorithms and suitable for the security of small data. However, these schemes cannot secure multimedia data like digital images, audio, and video data. To cover the issue of digital image security, numerous authors present image encryption schemes proposed based on nonlinear dynamical systems. These schemes are usually based on low and high-dimension chaotic sequences. The low dimensional chaotic sequence schemes have enough security issues due to low accuracy and short cord period. Thus, researchers pay attention to using high-dimensional chaotic sequences for the encryption algorithm[103]–[106]. Therefore, researchers used different mathematical structures to develop a secure image encryption scheme with minuscule computational complexity.

The cryptosystems-based elliptic curve has excellent cryptographic properties, hence widely used for secure communication. In [107], it presents an image encryption scheme using a fast-mapping method based on a matrix approach for ECC. In the proposed work, the authors used different properties of the matrix and elliptic curve to convert the alphanumeric character values to the elliptic curve coordinate (x, y) using the non-singular matrix. The mapping technique used in the scheme increases the security strength of the cryptosystem. However, the suggested encoding scheme's computational complexity (CC) is still high.

Generally, the generation of EC points is a time-consuming procedure, and overall, it affects the computational time; hence, there is an urge for the method to generate EC points comparatively fast. In addition, the conventional conversion of EC points into (x, y) points also influences the computational complexity, so conversion demands an effective and efficient procedure.

Keeping the above facts in view, this chapter introduced a novel symmetric key encryption algorithm based on the efficient computation of elliptic curve isomorphism(ECI) and 4-bit substitution boxes(S-Boxes) for the application of grayscale image encryption. In the first phase, the proposed algorithm utilized the searching technique to generate the points of EC, which reduces the complexity up to an exceptional margin. After that, the kobtliz encoding technique was employed to convert the plain image least significant bits(LSB) data to EC points. These points are then mapped to the isomorphic curve and are the reason for diffusion in the ciphertext. Besides this diffusion mechanism, elliptic curve points are also involved in constructing small substitution boxes for confusion. This proposed confusion and diffusion technique also provide quality security in response to well-known cryptographic attacks, as established by the number of statistical results and security analyses.

5.1 Koblitz Encoding

Nill Kobltiz in [108] first proposed the concept of representing plain data in the EC point. Consider the elliptic curve E, which is defined as: $y^2 = x^3 + \mathrm{A}x + \mathrm{B}$ over F_p. Let M, be the plain data, represent the value in the interval $0 \leq M < {}^{p}/_{100}$. Let $x_i = 100M + i$ for $0 \leq i < 100$. For $i = 0,1, \dots, 99$, calculate the value of $S_i = {x_i}^3 + \mathrm{A}x_i + \mathrm{B}$. If ${S_i}^{S(p-1)/2} \equiv 1 \bmod p$, then S_i is square mod p, in such a scenario, we don't need to check any more values of i. In the second case, if $p \equiv 3mod\ 4$, the square root S_i is given by $y_i = {S_i}^{(p+1)/4} \bmod p$. Finally, if $p \equiv 1mod\ 4$, it is also possible to compute the square root of S_i, although the process is more complex and hence we get the transform point of EC (x_i, y_i). The decoding procedure is effortless; compute the $\left\lfloor \frac{x_i}{100} \right\rfloor$ (= the greatest integer less than or equal to $\frac{x_i}{100}$). The execution time of the encoding processes depends on the parameters. However, the decoding time is independent of the parameters of the elliptic curve.

5.2 Isomorphic Elliptic Curve

Definition 5.1. Two elliptic curves over the field F_p given by the short Weierstrass equation

$$E_1 = y^2 = x^3 + \mathrm{A}x + \mathrm{B} \tag{5.1}$$

$$E_2 = y^2 = x^3 + \mathrm{C}x + \mathrm{D} \tag{5.2}$$

with $\mathrm{A}, \mathrm{B}, C, D \in F_p$ is said to be isomorphic if there exists $\beta \in F_p$ such that $C = \beta^4\mathrm{A}$ and $D = \beta^6\mathrm{B}$ we say that E_1 and E_2 are isomorphic. The morphism between the elliptic curve is

$$\gamma: (x, y) \to (\beta^2 x, \beta^3 y) \tag{5.3}$$

$$(\beta^{-2}x, \beta^{-3}y) \leftarrow (x, y): \varphi \tag{5.4}$$

5.3 S-Box Construction Algorithm

In the proposed scheme, we employed the S-box to produce confusion in the plain image. The S-box construction scheme consists of the following steps.

1. Initially, choose a prime number p and two distinct elements such that $A_1, A_2 < p$.
2. The prime number is selected such that the corresponding elliptic curve $E_p(A_1, A_2)$ have at least 6×16 points.
3. In the third step, generate the points of the elliptic curve using the equation given as follows.

$$y^3 = x^3 + A_1x + A_2 \; mod \;\; p$$

4. In the next step, add the x and y coordinates of each point of the elliptic curve and obtain a new set $E_{p,z}(A_1, A_2)$.

$$E_{\,p,z}(A_1, A_2) = \{z \mid z = x + y; (x, y) \in E_p\,(A_1, A_2)\} \tag{5.5}$$

Finally, we carried out the mod operation ${E_{p,z}}^{16}(A_1, A_2)$ to restrict the range of the elements of the set ${E_{p,z}}^{16}(A_1, A_2)$, into [0-16] and pick the first sixteen elements from the set, subsequently converting the elements into the 4×4 lookup table, which is the required S-box, as depicted in Table 34. Moreover, the evaluation criteria of the newly generated s-box based on the elliptic curve are given in table 35.

Table 34. Proposed Dyamnmic S-box based on Elliptic curve

5	2	8	15		5	8	2	11
14	13	1	6		0	6	15	12
0	12	11	9		1	3	9	13
4	3	10	7		4	10	14	7
S-box 1. $E_{173,16}(0,1)$					S-box 2. $E_{211,16}(0,1)$			
5	8	14	10		5	12	2	15
0	12	3	13		0	8	4	7
1	7	15	11		14	10	6	13
6	4	9	2		9	11	3	1
S-box 3. $E_{179,16}(0,1)$					S-box 4. $E_{251,16}(0,1)$			

5.4 Proposed Encryption Scheme

In this section, we discussed the proposed encryption algorithm. Let I denote the plain image of dimension $M \times N$ containing the element from the set $[0 - 255]$. Subsequently, we split the pixels of the image into LSBs and MSBs and convert the MSBs into LSBs. Accordingly, one gets a new matrix I_s of dimension $2 \times M \times N$, contain the entries between $0 - 16$. Then we processed the matrix I_s over the servel steps. In the next subsection, we discussed the entire steps in detail.

Table 35. Experimental analysis of newly generated S-box

	Results									
S-Boxes	NL	SAC	LAP	DAP	BIC-SAC	LS	LBN	DBN	FP	OFP
$E_{173,16}(0,1)$	4	0.4922	0.2500	0.0625	0.2500	0	2	2	0	0
$E_{211,16}(0,1)$	4	0.4688	0.2500	0.0625	0.2500	0	2	2	1	0
$E_{179,16}(0,1)$	4	0.4922	0.3750	0.0625	0.2500	0	2	2	1	0
$E_{251,16}(0,1)$	4	0.5000	0.2500	0.0625	0.2500	0	2	2	1	0

5.4.1 Preprocessing

In the first step, while using elliptic curve cryptography, the pixels of the plain image should be converted into elliptic curve points. In the proposed work, we used the Kobltiz method to map the pixels of the matrix I_s, into the elliptic curve points [108]. Let c_i be an element of the matrix I_s, compute the output pair $(x_i,\ y_i)$ of the element c_i using the following map.

$$k\colon\ I_s \to E_p(a,b)$$

$$k(c_i) = (x_i, y_i)$$

$$x_i = c_i k + l \, mod\, p \tag{5.6}$$

$$y_i = \sqrt{{x_i}^3 + \mathrm{A}x_i + \mathrm{B}}\ \, mod\, p \tag{5.7}$$

Where $x_i = c_i k + l < p$ and $0 \le l < p$ and compute y_i, which satisfies equation(5.7). The failure probability of finding y_i is $\frac{1}{2^L}$. According to [109], $L = 30$ is enough to achieve the required transformation of the data.

5.4.2 Postprocessing

The decoding process of the plain image includes the decoding of the coordinate $(x_i,\ y_i)$ of the elliptic curve by computing $M = \lfloor (x-1)/k \rfloor$. The detailed procedure is given in the following example 5.2.

Example 5.2. Let us have an elliptic curve, and the parameters of the EC are as follows.

$$\mathrm{A} = 1, \mathrm{B} = -1, p = 503, k = 20$$

Let $M = 22$ be a plaintext, then $x = Mk + 1 \gg 22 \times 20 + 1 = 441$, Since $= x^3 + \mathrm{A}x + \mathrm{B}\ mod\ p$ is not a perfect square, so it carried out the same operation and put $l = 2$, i.e., $x = mk + 2 = 442$, which is again not a perfect square. So, we have to iterate the same procedure for the various value of l till the equation becomes a perfect square. The equation $x^3 + \mathrm{A}x + \mathrm{B}\ mod\ p$ is a perfect square for $l = 19$. Accordingly, the plaintext is converted into the elliptic curve point$(459, 475)$. To decode the plaintext, subtract 1 from the x and divide the output by k and round the answer; the process is given below.

$$\lfloor (459 - 1)/k \rfloor = 22$$

After the conversion of preprocessing step, which is explained in detail in the above example 5.2, the next step is to use the isomorphism of the elliptic curve map to alter the position of the elliptic curve points to produce diffusion. The mathematical representation is given below

$$\gamma_m : E_p(\mathrm{A}, \mathrm{B}) \to E_p(C, D)$$

$$\gamma_m((x_i, y_i)) = (x_i{}', y_i{}') \tag{5.8}$$

Where the pair (x, y) denotes the elliptic curve point. After the isomorphism of the elliptic curve map, the range of γ_m is decoded and converted back to the matrix I_k of range $[0 - 16]$ by using the decoding process as discussed below. Furthermore, we need to add the abovementioned isomorphism curves and apply the substitution process discussed in section 5.4. After this substitution process, the obtained S-boxes are applied to the matrix I_k ,and one can get a new matrix I_s. In the next step, split the matrix of dimension $M \times N$ into two matrices I_{s1} and I_{s2} of dimension $M \times N$, and convert the matrix I_{s1} into MSB and combine the MSB with LSB. So, the obtained image is the required encrypted image. The flow diagram of the proposed work is shown in Figure 28.

5.5 Security Analysis Of Encryption Scheme

Security analysis determines whether a cryptosystem is good enough to counter malicious attacks. For good encryption, it should resist all kinds of known attacks. Moreover, in this section, most security analysis results are discussed in chapter 2, so we just show their graphical and tabular representation, not their theoretical description. The simulations take a data set of input images, Lena, baboon, fruit, and pepper. Figure 29 shows the above data set, plain and encrypted images. It can be envisaged from the encrypted image that encryption results are visually strong.

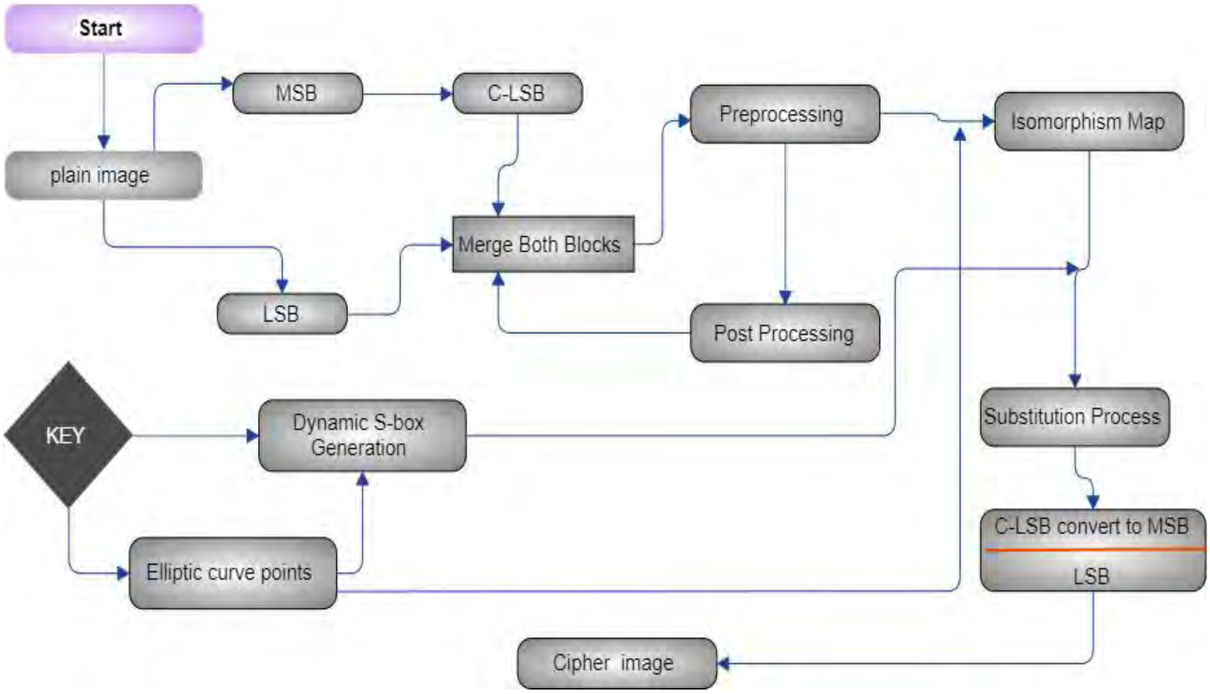


Figure 28. Flow Chart of the Proposed algorithm

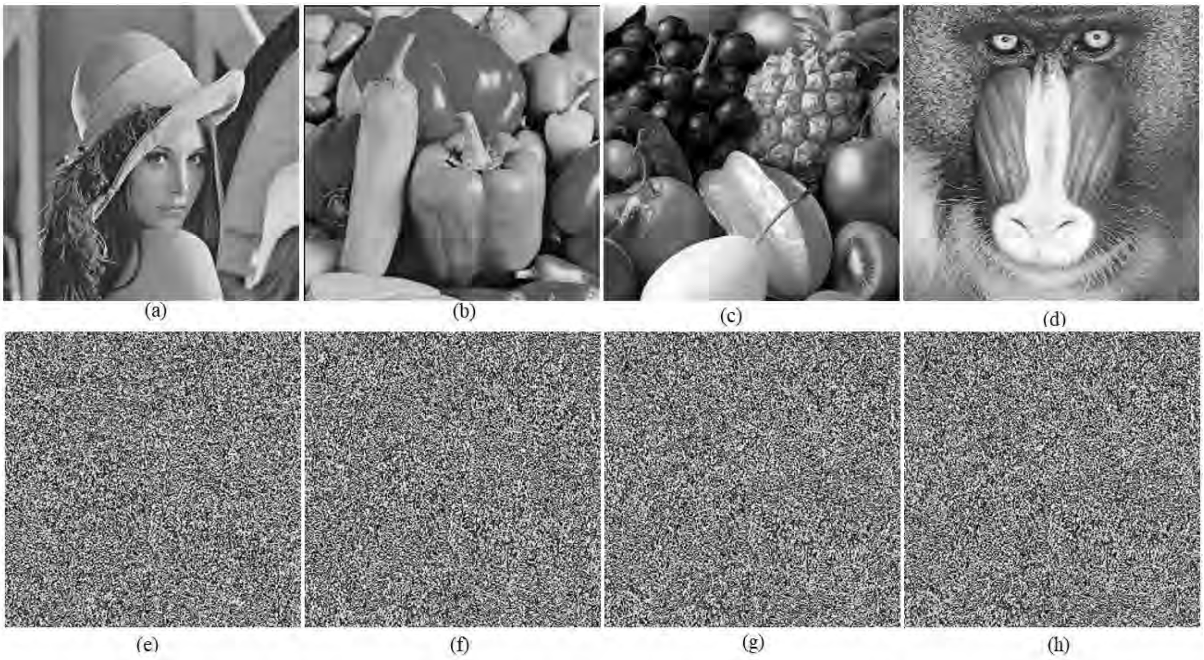


Figure 29. (a-d)Plan image of Lena, Fruit, Peppers, and Baboon from (e-h) their cipher images, respectively

5.5.1 Histogram Variance Analysis

Histogram variance analysis is considered a quantitative measurement of the histogram. The low value of variance represents the high-level uniformity of a grayscale image; inversely, the low uniformity of a grayscale image shows a high variance value. The histogram variance value is defined in equation (5.9) [110].

$$V(X) = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{(x_i-x_j)^2}{2} \tag{5.9}$$

where N is the grayscale value, and x_i,x_j , represents the pixels of grayscale values, respectively. Table 36 shows the histogram variance result of some grayscale test images of size 256×256. Table 36 shows that the variance analysis of encrypted images is highly dissimilar from plain images. The results of decrypted images using our proposed scheme are almost equal to plain images. These high differences between encrypted and plain images ensure that the histogram variance analysis of grayscale values is highly uniform.

Table 36. Variance analysis

Image	Original	Encrypted image	Decrypted image
Lena	38952	256.8324	38952
Baboon	38871	279.9321	38871
Peppers	480,660	260.2344	480,660
Fruit	11,787	250.0551	11,787

5.5.2 Chi-Square test

The Chi-square test is the degree of variance among original sample data and the theoretical inference value of the statistical samples. The chi-square is less appropriate if the value is larger; on the contrary, a less value of the Chi-square represents more consistency. The chi-square test values will be 0 if the two values are the same, showing that high grayscale uniformity and the theoretical value are more consistent. The mathematical formula of the Chi-square metric is given in equation (5.10-5.11) [111].

$$\mathcal{X}^2 = \sum_{i=0}^{255}\frac{(ob(f_i)-ex(f_0))}{ex(f_0)} \tag{5.10}$$

$$ex(f_0) = \frac{(M\times N)}{256} \tag{5.11}$$

Where $ob(f_i)$ is the observed frequency $i(i = o\ to\ 255)$, while $ex(f_0)$, is the expected frequency. Table 37 represents the Chi-square test results of cipher images. According to the chi-square distribution table, $\mathcal{X}^2{}_{255,0.01} = 310.457$ and,$\mathcal{X}^2{}_{255,0.05} = 293.2478$, ensure that the hypothesis of the chi-square test is accepted and the significant level for both values is 1% and 5%, respectively. From this, we can say that the distribution of pixels is uniform.

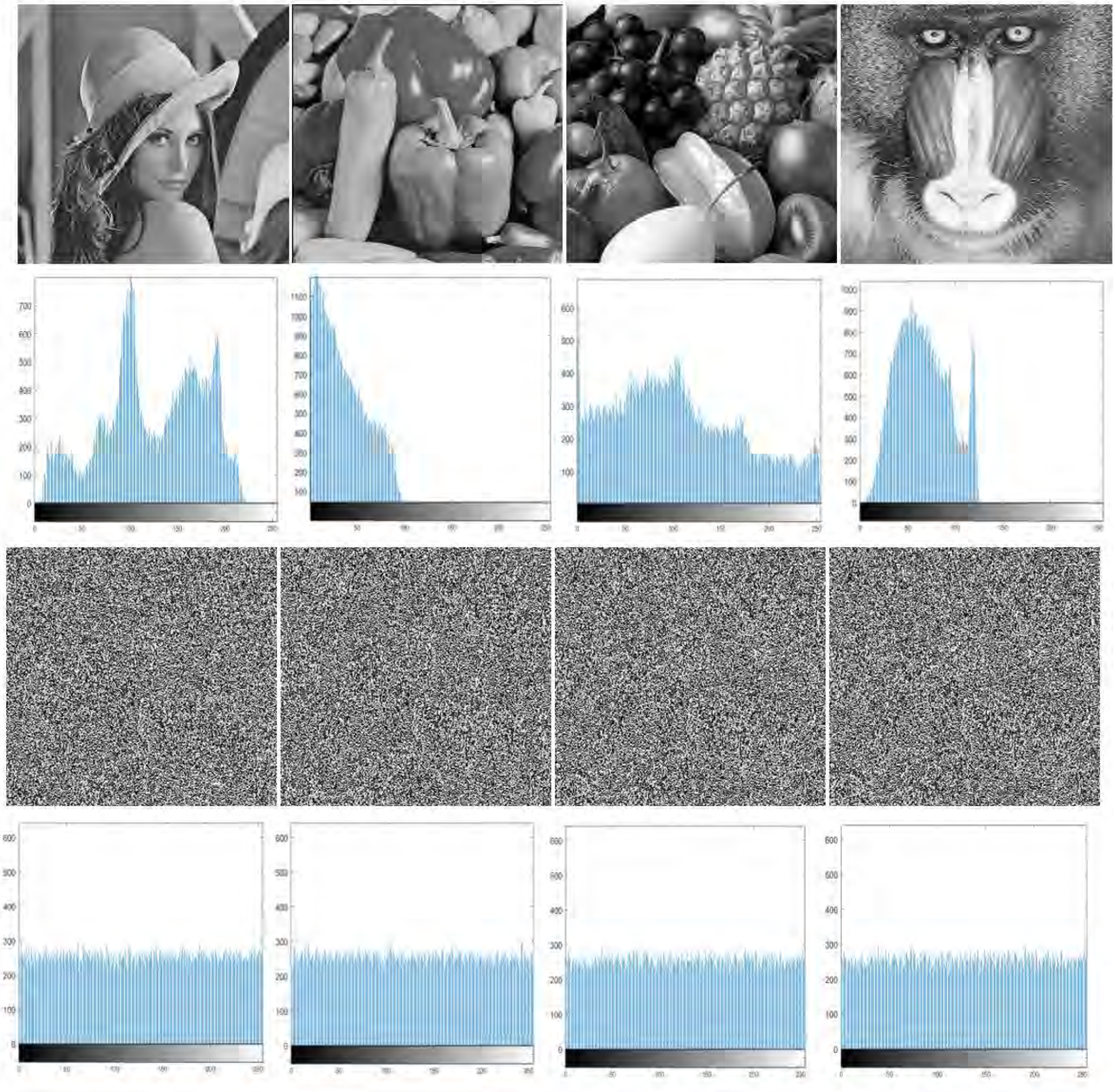


Figure 30. Histogram analysis of the original image Lena and corresponding their encrypted image histogram

Table 37. Result of Chi-square test

Images	$\mathcal{X}^2{}_{Test}$	Result
Lena 256 × 256	234.1314	Success
Baboon 256 × 256	236.2627	Success
Fruit 256 × 256	235.2312	Success

5.5.3 Binary Image Test

Binary image test to measure that our proposed algorithm works well on binary images. We tested the different binary images, and the outcomes are shown in the Figure. 31. It can be seen that the conventional methods do not usually work properly on binary images. But our proposed algorithm works well on black-and-white binary images, which ensures that our proposed algorithm works well on binary images.

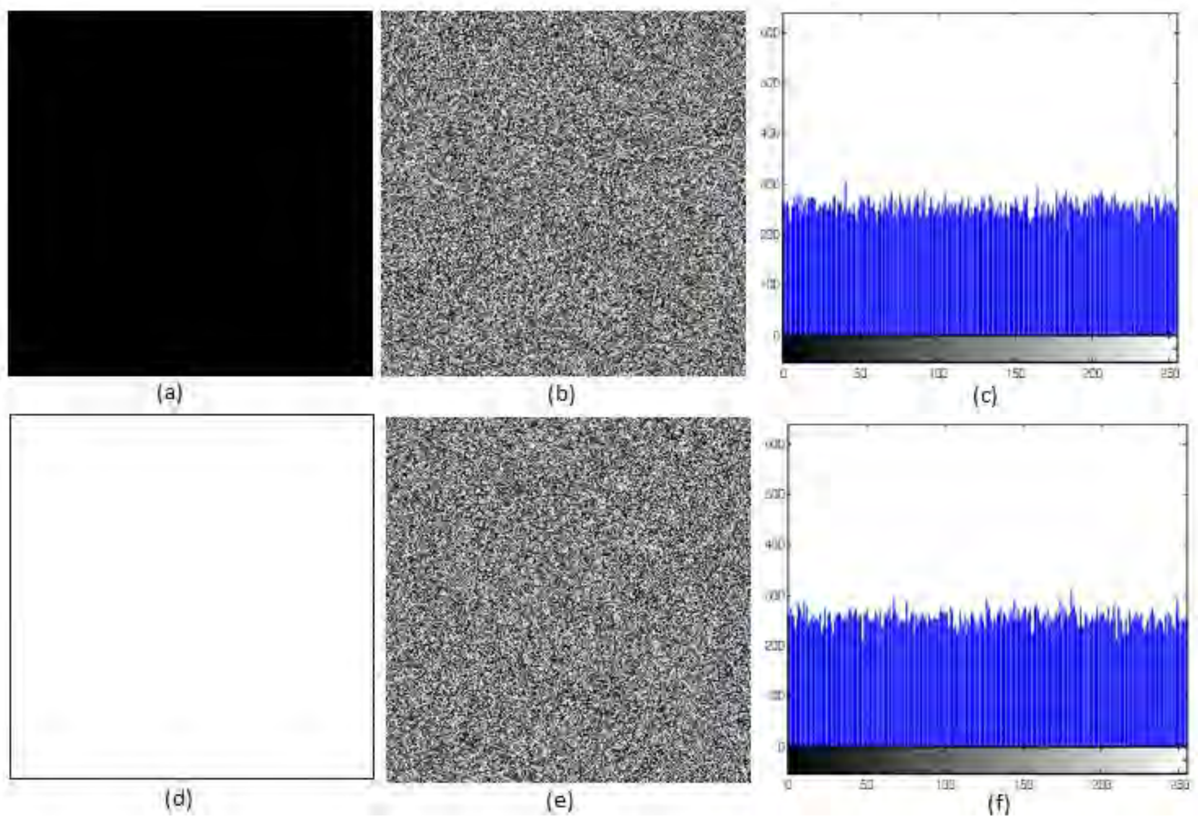


Figure 31. Binary White and Black image analysis

5.5.4 Local Shannon Entropy

Sometimes, cipher image blocks have very low entropy information [112]. In this scenario, the proposed encryption algorithm will not be considered highly secure. The Local Shannon entropy computes the extracted randomness of pixel values in the cipher image. We can define the local Shannon entropy for the block of cipher image as [113].

$$\overline{\boldsymbol{H}_{\boldsymbol{K},\boldsymbol{T_B}}}(S) = \sum_{i=1}^{K} \frac{H(S_i)}{K} \tag{5.12}$$

where S_i $(i = 1 \dots\dots, k)$ are non-overlapping blocks with randomly chosen pixels $\boldsymbol{T_B}$ of cipher image and $H(S_i)$ express the entropy information of $S_1, S_2, S_3, \dots\dots\dots, S_K$. For the local Shannon entropy test, we select k images and $\boldsymbol{T_B}$ pixels and $K = 30, \boldsymbol{T_B} = 1936$. The range of $K = 30, \boldsymbol{T_B} = 1936$ should be from $[7.901901305 - 7.903037329]$, with a significance level of 0.05. Table 38, represents the information on local Shannon entropy, showing that the cipher image results possess high randomness.

Table 38. Entropy information

Image	Test values	Result
Lena	7.9029	Pass
Baboon	7.9028	Pass
Paper’s	7.9028	Pass
Monogram	7.9024	Pass

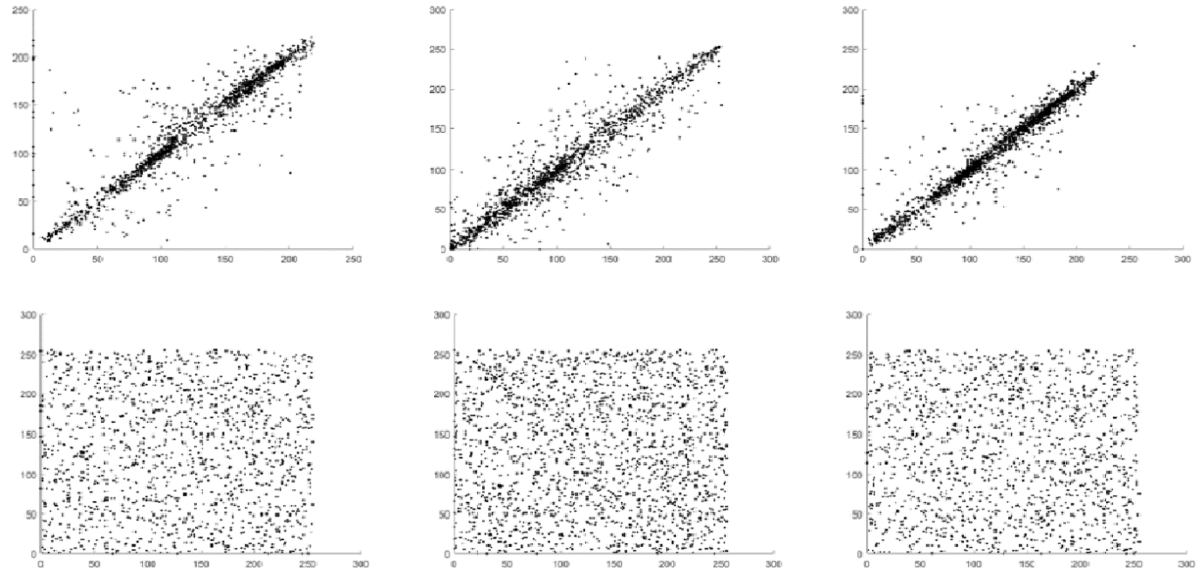


Figure 32. Correlation analysis in Horizontal, Vertical and Diagonal for original image Lena and corresponding their encrypted image

Table 39. Information of the correlation of proposed schemes

Images	Horizontal correlation	Vertical correlation	Diagonal correlation
Lena plan-image	0.9437	0.9705	0.9089
Lena-cipher image	−0.0090	−0.0079	−0.0032
Baboon plan-image	0.9537	0.9781	0.8821
Baboon cipher image	−0.0081	0.0021	0.0031
Peppers plan-image	0.9467	0.9725	0.9651
Peppers cipher image	−0.0003	−0.0003	0.0008
Fruit plan-image	0.9537	0.9864	0.9845
Fruit cipher image	0.0002	−0.0061	−0.0016

5.5.5 Key Space Analysis

Better encryption and decryption security are built upon the key size used. The larger the key size, the harder it is to perform an attack using the Brute Force attack. Commonly a cryptosystem fascinates the key space analysis if it has the key spacing more than 2^{100}. In our proposed algorithm, we have used a 512-bit; this implies that the key spacing analysis of our proposed algorithm is much larger than 2^{100}. Hence, the proposed encryption technique resists brute-force attacks efficiently. We used nine(9) keys $\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{A}_1, \mathrm{A}_2, p\ , k, and\ \beta$ and each of these nine keys by 512-bit; this implies that the key spacing analysis of our proposed algorithm is much larger than 2^{100}.

5.6 Computational Complexity of The Algorithm

The computational complexity of the scheme is the number of bit operations required for the algorithm to be Completed. In this section, we discussed the computational complexity of the proposed scheme. The scheme initially split the image into MSBs and LSBs. The scheme splits each image pixel into two sub-blocks in constant time $O(1)$. Thus, the first required $O(M \times N)$ bit operation is to split the complete image into MSBs and LSBs. Afterwards, the scheme maps the elements of the image into the points of the elliptic curve. The scheme maps each element of the image in constant time as the data of the image lay in the fixed range. Therefore, the preprocessing requires $O(M \times N)$ bit operations to execute. Similarly, the substitution module is also performed in linear time. Since all algorithm modules run in linear time, the proposed scheme's computational complexity is $O(M \times N)$ linear time, where $M \times N$ is the dimension of the plain image.

Table 40. Time execution

	Prime	A	B	Preprocessing Timing	Post Processing Timing
Proposed	4093	9	7	0.110 sec	0.000002sec
Proposed	16381	1	17	2.4567sec	0.000002sec
Ref.[108]	16381	1	17	3.7sec	0.000002sec
Ref. [108]	4093	9	7	1.11sec	0.000003sec

5.7 Comparison And Discussion With Other Encryption Techniques

The Comparison of our proposed encryption algorithm with other existing cryptosystems based on a different mathematical structure, like a chose-based and elliptic curve [104]–[106] [108], is presented in this subsection. The scheme proposed in [108] converts the message encoding and decoding into the elliptic curve coordinate using the Kobltiz method and describes the implementation results of Kobltiz's Encoding and Decoding methods. While our proposed scheme is based on image encryption, every pixel of the plain image is considered a massage. The execution timing of massage m converted to (x, y) is less than the existing scheme, and the execution time in [108] is taken more time than the proposed Technique; the execution timing of ref [108] is listed in Table 41. The comparative analysis of the proposed encryption algorithm with recent encryption schemes is discussed in the following points.

Table 41. Comparison table with other existing schemes

Scheme	NPCR	UACI	Entropy	Hor-C	Vert-C	Diag-C	Variance Analysis	$\mathcal{X}^2$
Proposed	99.6634	33.7112	7.997	−0.0090	−0.0079	−0.0032	256.8324	234.13
Ref. [104]	99.6233	33.4766	7.999	−0.0034	0.0019	−0.0134	-	-
Ref.[114]	99.6228	33.7041	7.996	−0.0048	−0.0112	−0.0045	-	-
Ref.[113]	99.6166	33.4365	7.999	0.0018	0.0011	−0.0012	-	-
Ref.[115]	99.4186	33.1670	7.957	−0.0083	0.0458	−0.0528	-	-
Ref.[116]	99.6093	33.4723	7.997	0.00152	0.0013,	0.0018	-	-
Ref.[117]	99.6143	33.5513	7.999	0.0031	0.0005	-0.0041	969.5729	-
Ref.[111]	99.6109	33.4783	7.997	0.0008	-0.0019	-0.0016	676.8	233.13
Ref.[118]	99.6198	33.4777	7.997	−0.0056	0.0028	−0.001	265.8906	-
Ref.[119]	99.6216	33.5848	7.997	-0.0056	0.0006	0.0018	250.6719	-
Ref.[120]	99.6216	33.4994	7.997	0.0106	-0.0012	0.009	-	253.48
Ref.[121]	90.1978	30.0263	7.989	-0.0015	-0.0143	-0.0236	310.44	-

1. From Table 41, we can see that the results of the proposed cryptosystem's differential attack analysis (NPCR and UACI) are better than the other excellent existing algorithm [116] [117] [111] [118] [119] [120] [121].
2. The entropy information of the proposed algorithm is nearly equal to 8, which shows more randomness of pixel values by using the proposed cryptosystem. This can be seen by comparing other cryptosystems[114] [115] [120] [121] and having less randomness than [104] [113] [117].
3. By observing the correlation analysis, the value of the correlation coefficient is nearly close to zero, which ensures that the proposed cryptosystem outperforms and is robust against statistical attack compared to other encryption schemes [115] [120] and somehow less or equal to[116] [117] [119] [121] .
4. The histogram variance analysis results of the proposed encryption algorithm in Table 41 are comparatively less than the current existing encryption method in[117] [111] [118][119] [121]. This proves that the pixels of cipher images are largely uniform.
5. The $\mathcal{X}^2{}_{Test}$, the test analysis result of our method is less as compared to the chi-square value of [120] and greater than[111], which shows that the proposed work has high gray scale uniformity.

Chapter 6

Conclusion and Future Work

This thesis illustrates the significant rule of an elliptic curve over a finite field in a symmetric and hybrid architecture for the application of multimedia data security. This chapter summarises the main finding of the thesis. Further development and future scope are also discussed at the end of this chapter.

6.1 Summary of Thesis

This thesis presents the importance of the application and theory of efficient computation of elliptic curve cryptography. In this thesis, different cryptosystems are built on the core mathematics of elliptic curves over a finite field for multimedia data security. Furthermore, the EC over a finite field, the arithmetic of point generation, has been effectively utilized for the symmetric and integrated encryption scheme. Moreover, each chapter of the thesis follows the Substitution Permutation Network(SPN) design, intending to increase security and perform strong pseudorandom number permutation.

The second chapter reviewed the Elliptic Curve Integrated Encryption Scheme(ECIES) over a finite field. Based on the hard problem of the discrete log problem of the elliptic curve, we designed the enhanced version of the elliptic curve integrated encryption scheme (E-ECIES). From the shared key at the initial stage of the algorithm, we extracted the new symmetric key for the application of RGB image encryption. The suggested approach of the symmetric encryption scheme achieves the aim of diffusion using the first twelve bytes of the symmetric key of 128 bits. The confusion module is accomplished by the affine power affine transformation(APA) followed by the last four bytes of the symmetric. Furthermore, after comparing the proposed encryption scheme with other excellent existing cryptosystems, we can observe that the statistical and sensitivity analysis of the proposed algorithm offers perfect security and can withstand common attacks.

In chapter 3, we present a unique lossless audio encryption scheme with Substitution Permutation Architecture (SPA) based on efficient computation of the Mordell elliptic curve (MEC) over a finite field for real-world communications. At the first stage of the algorithm, generate the strong pseudorandom number generation using MEC to achieve the diffusion of the audio data. In addition, the inclusion of substitution boxes is involved in the confusion phase. The substitution with multiple 5×5 bijective S-boxes eventually produces optimum confusion in encrypting each 5-bit data block, ensuring the proposed algorithm is robust against differential attacks. The simulation result presents that the suggested encryption efficiently encrypts and turns the audio data into indistinguishable uniform audio data. Accordingly, the proposed scheme is securely suitable for real-world communication.

Chapter 4 presents an efficient digital watermarking encryption scheme based on HEC. The proposed scheme is key-dependent, and only the main owner of the image can prove his ownership using his secret key. The proposed scheme uses random sequences generated through the HEC and distributes the watermark image data randomly. On the one hand, the random distribution of the watermark image does not impact the quality of the host image; on the other hand, this approach enhances the security of the proposed scheme, as only the authorized owner can reproduce the watermark image. Furthermore, after comparing the proposed watermarking scheme with other excellent existing cryptosystems, we can observe that the experimental findings of the proposed algorithm offer perfect security and can withstand common attacks.

The efficient computation of elliptic curves and small substitution boxes is present in chapter five. The proposed scheme utilizes the searching method to generate EC points, which reduces the complexity to an exceptional margin. After that, the proposed algorithm follows the substitution permutation network(SPN); the permutation is attained through the isomorphism of the elliptic curve map, and the small S-boxes are utilized for the confusion of the data. The substitution layer evaluates by their stand of the art analysis, and we have found it secure against linear and differential attacks. Over several simulation assessments, the proposed scheme has been extensively securitized. The outcomes of the simulation experiment have demonstrated that the suggested scheme is resistant to several cryptanalysis techniques. The recommended approach is, therefore, safely appropriate for grayscale and binary image encryption applications.

6.2 Future Work

The enhanced elliptic curve integrated encryption (E-ECIES) is present for the RGB image encryption. For future work, it would be fascinating to look into how the E-ECIES would be implemented on hardware and how it may be used for more multimedia applications like Telecare Medical Information Systems (TMIS) and the Internet of things (IoT).

Furthermore, the audio encryption scheme based on generating MEC points is time-consuming, and the algorithm's computational complexity is reasonably high. Therefore, the effort may be given to make this computation efficient for a strong random number generation scheme with less computational complexity in the future. Moreover, the nonlinear layer S-box has some fixed points due to its random behaviour; therefore, the fixed points may be removed as the area for future scope. The proposed algorithm is validated for offline audio files, although live encrypted audio streaming is in demand these days. Thus, in the future, an attempt may be made to speed up this algorithm to expand the use of this application for live audio streaming.

The grayscale image encryption is based on the fusion of isomorphism of an elliptic curve and small S-box, presented in this thesis. Since, in the proposed work, the prime p is entirely dependent on the image dimension, therefore in the case of large image data, it is time-consuming, and for small images, the key space remains small, which cannot resist the brute force attack. We may extend this proposed work for audio and video encryption applications in the future and utilize it for the application of the Internet of things(IoT).

References

[1] Guide to elliptic curve cryptography. New York: Springer-Verlag, 2004.

[2] L. C. Washington, Elliptic curves: number theory and cryptography. Chapman and Hall/CRC, 2008.

[3] D. Husemöller, "Elliptic Curves over Finite Fields," Elliptic Curves, pp. 253–273, 2004.

[4] H. Cohen et al., Handbook of elliptic and hyperelliptic curve cryptography. CRC press, 2005.

[5] A. Stein, "Hyperelliptic curves and cryptography," High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, vol. 41, p. 255, 2004.

[6] J. Scholten and F. Vercauteren, "An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU," 2008.

[7] D. Mumford, Curves and their Jacobians. Ann Arbor: University of Michigan Press, c1975, 1976 printing., 1975.

[8] W.-L. Chow, S.-S. Chern, and V. V. Shokurov, The Collected Papers of Wei-Liang Chow, vol. 8. World Scientific, 2002.

[9] C. Guyot, K. Kaveh, and V. M. Patankar, "Explicit algorithm for the arithmetic on the hyperelliptic Jacobians of genus 3," Journal-Ramanujan Mathematical Society, Vol. 19, No. 2, Pp. 75–115, 2004.

[10] N. Koblitz, "Hyperelliptic cryptosystems," Journal of cryptology, vol. 1, no. 3, pp. 139–150, 1989.

[11] An introduction to mathematical cryptography. New York, NY: Springer New York, 2008.

[12] O. Shevchuk, "Introduction to Elliptic Curve Cryptography," 2020.

[13] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," Signal Processing, vol. 125, pp. 187–202, Aug. 2016, doi: 10.1016/j.sigpro.2016.01.017.

[14] R. R. Ahirwal and M. Ahke, "Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network," International Journal of Computer Science and Information Technologies, vol. 4, no. 2, pp. 363–368, 2013.

[15] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–203, Jan. 1987, doi: 10.1090/S0025-5718-1987-0866109-5.

[16] G. Baumslag, B. Fine, M. Kreuzer, and G. Rosenberger, A course in mathematical cryptography. Berlin, München, Boston: DE GRUYTER, 2015.

[17] R. A. Mollin, An introduction to cryptography. Chapman and Hall/CRC, 2006.

[18] B. Schneier, “Applied cryptography protocols algorithms and source code in C,” 1996.

[19] L. Liu, Z. Zhang, and R. Chen, “Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos,” IEEE Access, vol. 7, pp. 126450–126463, 2019.

[20] C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[21] F. Ö. Catak and A. F. Mustacoglu, “CPP-ELM: cryptographically privacy-preserving extreme learning machine for cloud systems,” International Journal of Computational Intelligence Systems, vol. 11, no. 1, p. 33, 2018.

[22] F. O. Catak, I. Aydin, O. Elezaj, and S. Yildirim-Yayilgan, “Practical implementation of privacy preserving clustering methods using a partially homomorphic encryption algorithm,” Electronics, vol. 9, no. 2, p. 229, 2020.

[23] A. A. Abd El-Latif and X. Niu, “A hybrid chaotic system and cyclic elliptic curve for image encryption,” AEU - International Journal of Electronics and Communications, vol. 67, no. 2, pp. 136–143, Feb. 2013, doi: 10.1016/j.aeue.2012.07.004.

[24] M. Abdalla, M. Bellare, and P. Rogaway, “The oracle Diffie-Hellman assumptions and an analysis of DHIES,” in Cryptographers Track at the RSA Conference, 2001, pp. 143–158.

[25] M. Benssalah, Y. Rhaskali, and K. Drouiche, “An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography,” Multimedia Tools and Applications, vol. 80, no. 2, pp. 2081–2107, 2021.

[26] S. D. Galbraith and P. Gaudry, “Recent progress on the elliptic curve discrete logarithm problem,” Des. Codes Cryptogr., vol. 78, no. 1, pp. 51–72, Jan. 2016, doi: 10.1007/s10623-015-0146-7.

[27] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, “A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2,” Nonlinear Dyn., vol. 83, no. 3, pp. 1123–1136, Feb. 2016, doi: 10.1007/s11071-015-2392-7.

[28] L. Cui and Y. Cao, “A new S-box structure named affine-power-affine,” International Journal of Innovative Computing, Information and Control, vol. 3, no. 3, pp. 751–759, 2007.

[29] M. Khan and Z. Asghar, “A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation,” Neural Comput & Applic, vol. 29, no. 4, pp. 1–7, Aug. 2016, doi: 10.1007/s00521-016-2511-5.

[30] N. A. Azam, U. Hayat, and M. Ayub, “A substitution box generator, its analysis, and applications in image encryption,” Signal Processing, vol. 187, p. 108144, 2021.

[31] U. Hayat, I. Ullah, N. A. Azam, and S. Azhar, “A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings,” Entropy, vol. 24, no. 5, p. 571, 2022.

[32] M. I. Haider, A. Ali, D. Shah, and T. Shah, “Block ciphers nonlinear component design by elliptic curves: an image encryption application,” Multimedia Tools and Applications, vol. 80, no. 3, pp. 4693–4718, 2021.

[33] A. Javeed, T. Shah, and A. Ullah, “Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group,” Wireless Personal Communications, vol. 112, no. 1, pp. 467–480, 2020.

[34] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, “A novel scheme of substitution-box design based on modified Pascals triangle and elliptic curve,” Wireless Personal Communications, vol. 116, no. 4, pp. 3015–3030, 2021.

[35] F. Masood et al., “A new color image encryption technique using DNA computing and Chaos-based substitution box,” Soft Computing, vol. 26, no. 16, pp. 7461–7477, 2022.

[36] F. Artuger and F. Özkaynak, “An effective method to improve nonlinearity value of substitution boxes based on random selection,” Information Sciences, vol. 576, pp. 577–588, 2021.

[37] D. Lambic, “A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design,” Nonlinear Dynamics, vol. 100, no. 1, pp. 699–711, 2020.

[38] J. Daemen and V. Rijmen, “AES proposal: Rijndael,” 1999.

[39] N. Sasikaladevi, K. Geetha, K. Sriharshini, and M. D. Aruna, “H3-hybrid multilayered hyper chaotic hyper elliptic curve based image encryption system,” Optics & Laser Technology, vol. 127, p. 106173, 2020.

[40] S. Farwa, N. Bibi, and N. Muhammad, “An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling,” Multimedia Tools and Applications, vol. 79, no. 37, pp. 28225–28238, 2020.

[41] J. Wu, X. Liao, and B. Yang, “Color image encryption based on chaotic systems and elliptic curve ElGamal scheme,” Signal Processing, vol. 141, pp. 109–124, Dec. 2017, doi: 10.1016/j.sigpro.2017.04.006.

[42] C. Carlet and C. Ding, “Nonlinearities of S-boxes,” Finite fields and their applications, vol. 13, no. 1, pp. 121–135, 2007.

[43] P. P. Mar and K. M. Latt, “New analysis methods on strict avalanche criterion of S-boxes,” World Academy of Science, Engineering and Technology, vol. 48, no. 150–154, p. 25, 2008.

[44] M. Matsui, “Linear cryptanalysis method for DES cipher,” in Workshop on the Theory and Application of of Cryptographic Techniques, 1994, pp. 386–397.

[45] H. D. Tho, N. T. Thang, N. T. T. Nga, and P. Q. Hoang, “An Algorithm for Improving Algebraic Degree of S-Box Coordinate Boolean Functions Based on Affine Equivalence Transformation,” Jour. Inform. Math. Sci., vol. 10, no. 1–2, pp. 339–350, Aug. 2018, doi: 10.26713/jims.v10i1-2.662.

[46] S. Sarkar and H. Syed, “Bounds on differential and linear branch number of permutations,” in Information security and privacy, vol. 10946, W. Susilo and G. Yang, Eds. Cham: Springer International Publishing, 2018, pp. 207–224.

[47] C.-K. Wu, D. Feng, and Others, Boolean functions and their applications in cryptography. Springer, 2016.

[48] H. Liang, G. Zhang, W. Hou, P. Huang, B. Liu, and S. Li, “A Novel Asymmetric Hyperchaotic Image Encryption Scheme Based on Elliptic Curve Cryptography,” Applied Sciences, vol. 11, no. 12, p. 5691, 2021.

[49] N. Bhosale, R. Manza, and K. V. Kale, “Analysis of effect of Gaussian, salt and pepper noise removal from noisy remote sensing images,” 2014.

[50] P. Arulpandy and M. T. Pricilla, “Speckle noise reduction and image segmentation based on a modified mean filter,” Computer Assisted Methods in Engineering and Science, vol. 27, no. 4, pp. 221–239, 2020.

[51] S. W. Hasinoff, “Photon, Poisson Noise.,” Computer Vision, A Reference Guide, vol. 4, 2014.

[52] Q. Lai, H. Zhang, P. D. K. Kuate, G. Xu, and X.-W. Zhao, “Analysis and implementation of no-equilibrium chaotic system with application in image encryption,” Applied Intelligence, pp. 1–24, 2022.

[53] L. Xu, Z. Li, J. Li, and W. Hua, “A novel bit-level image encryption algorithm based on chaotic maps,” Opt. Lasers Eng., vol. 78, pp. 17–25, Mar. 2016, doi: 10.1016/j.optlaseng.2015.09.007.

[54] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption,” Signal Processing, vol. 160, pp. 45–58, Jul. 2019, doi: 10.1016/j.sigpro.2019.02.016.

[55] X. Wang and S. Gao, “Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory,” Information sciences, vol. 507, pp. 16–36, 2020.

[56] B. Jasra and A. H. Moon, “Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system,” Expert Systems with Applications, vol. 206, p. 117861, 2022.

[57] L.-L. Huang, S.-M. Wang, and J.-H. Xiang, “A tweak-cube color image encryption scheme jointly manipulated by chaos and hyper-chaos,” Applied Sciences, vol. 9, no. 22, p. 4854, 2019.

[58] M. Zarebnia, H. Pakmanesh, and R. Parvaz, “A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images,” Optik (Stuttg), vol. 179, pp. 761–773, Feb. 2019, doi: 10.1016/j.ijleo.2018.10.025.

[59] A. Girdhar, H. Kapur, and V. Kumar, “A novel grayscale image encryption approach based on chaotic maps and image blocks,” Applied Physics B, vol. 127, no. 3, pp. 1–12, 2021.

[60] S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, and S. Gao, “A novel image encryption cryptosystem based on true random numbers and chaotic systems,” Multimedia Systems, vol. 28, no. 1, pp. 95–112, 2022.

[61] C. M. Kumar, R. Vidhya, and M. Brindha, “An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function,” Applied Intelligence, vol. 52, no. 3, pp. 2556–2585, 2022.

[62] Z. Bashir, M. G. Malik, M. Hussain, and N. Iqbal, “Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol,” Multimedia Tools and Applications, vol. 81, no. 3, pp. 3867–3897, 2022.

[63] J. Daemen and V. Rijmen, “Reijndael: The advanced encryption standard.,” Dr. Dobb’s Journal: Software Tools for the Professional Programmer, vol. 26, no. 3, pp. 137–139, 2001.

[64] D. E. Standard and Others, “Data encryption standard,” Federal Information Processing Standards Publication, vol. 112, 1999.

[65] W. C. Barker and E. B. Barker, “Recommendation for the triple data encryption algorithm (TDEA) block cipher,” National Institute of Standards and Technology, Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-67r1.

[66] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[67] J. Pierce, “The early days of information theory,” IEEE Trans. Inform. Theory, vol. 19, no. 1, pp. 3–8, Jan. 1973, doi: 10.1109/TIT.1973.1054955.

[68] C. Li, Y. Zhang, and E. Y. Xie, “When an attacker meets a cipher-image in 2018: A year in review,” Journal of Information Security and Applications, vol. 48, p. 102361, 2019.

[69] J. Zhou and O. C. Au, “Security and efficiency analysis of progressive audio scrambling in compressed domain,” in 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, 2010, pp. 1802–1805.

[70] J. B. Lima and E. F. da Silva Neto, “Audio encryption based on the cosine number transform,” Multimed. Tools Appl., vol. 75, no. 14, pp. 8403–8418, Jul. 2016, doi: 10.1007/s11042-015-2755-6.

[71] H. Liu, A. Kadir, and Y. Li, “Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys,” Optik - International Journal for Light and Electron Optics, vol. 127, no. 19, pp. 7431–7438, Oct. 2016, doi: 10.1016/j.ijleo.2016.05.073.

[72] F. J. Farsana, V. R. Devi, and K. Gopakumar, “An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. Appl,” COMPUT. INFORM., TO BE PUBLISHED, DOI, vol. 10, 2019.

[73] M. A. Farah, R. Guesmi, A. Kachouri, and M. Samet, “A new design of cryptosystem based on S-box and chaotic permutation,” Multimedia Tools and Applications, vol. 79, no. 27, pp. 19129–19150, 2020.

[74] D. Shah, T. Shah, I. Ahamad, M. I. Haider, and I. Khalid, “A three-dimensional chaotic map and their applications to digital audio security,” Multimed. Tools Appl., vol. 80, no. 14, pp. 22251–22273, Jun. 2021, doi: 10.1007/s11042-021-10697-3.

[75] I. Khalid, S. S. Jamal, T. Shah, D. Shah, and M. M. Hazzazi, “A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes,” IEEE Access, vol. 9, pp. 77798–77810, 2021.

[76] S. Adhikari and S. Karforma, “A novel audio encryption method using Henon--Tent chaotic pseudo random number sequence,” International Journal of Information Technology, vol. 13, no. 4, pp. 1463–1471, 2021.

[77] H. Aziz, S. M. M. Gilani, I. Hussain, A. K. Janjua, and S. Khurram, “A Noise-Tolerant Audio Encryption Framework Designed by the Application of S8 Symmetric Group and Chaotic Systems,” Mathematical Problems in Engineering, vol. 2021, 2021.

[78] M. S. Khoirom, D. S. Laiphrakpam, and T. Tuithung, “Audio encryption using ameliorated ElGamal public key encryption over finite field,” Wireless Personal Communications, vol. 117, no. 2, pp. 809–823, 2021.

[79] P. K. Naskar, S. Bhattacharyya, and A. Chaudhuri, “An audio encryption based on distinct key blocks along with PWLCM and ECA,” Nonlinear Dynamics, vol. 103, no. 2, pp. 2019–2042, 2021.

[80] P. K. Naskar, S. Paul, D. Nandy, and A. Chaudhuri, “DNA encoding and channel shuffling for secured encryption of audio data,” Multimed. Tools Appl., vol. 78, no. 17, pp. 25019–25042, Sep. 2019, doi: 10.1007/s11042-019-7696-z.

[81] R. Apau and S. A. Gyamfi, “Data hiding in audio signals using elliptic curve cryptography, huffman code algorithm and low-bit encoding,” International Journal of Computer Applications, vol. 180, pp. 24–34, 2018.

[82] R. Shelke and M. Nemade, “Audio encryption algorithm using modified elliptical curve cryptography and arnold transform for audio watermarking,” in 2018 3rd International Conference for Convergence in Technology (I2CT), Apr. 2018, pp. 1–4, doi: 10.1109/I2CT.2018.8529329.

[83] A. K. Singh et al., “Guest editorial: robust and secure data hiding techniques for telemedicine applications,” Multimedia Tools and Applications, vol. 76, no. 5, pp. 7563–7573, 2017.

[84] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Dave, “Watermarking techniques and its applications in tele-health: A technical survey,” in Cryptographic and information security, CRC Press, 2018, pp. 467–508.

[85] A. K. Singh, “Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images,” Multimed. Tools Appl., vol. 76, no. 6, pp. 8881–8900, Mar. 2017, doi: 10.1007/s11042-016-3514-z.

[86] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, “Hiding clinical information in medical images: A new high capacity and reversible data hiding technique.,” J. Biomed. Inform., vol. 66, pp. 214–230, Jan. 2017, doi: 10.1016/j.jbi.2017.01.006.

[87] R. A. Asif, “Efficient computation for hyper elliptic curve based cryptography,” Electronic Theses and Dissertations. 5719., 2016.

[88] D. G. Cantor, “Computing in the Jacobian of a hyperelliptic curve,” Mathematics of computation, vol. 48, no. 177, pp. 95–101, 1987.

[89] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, “Comparative Study of Hyperelliptic Curve Cryptosystem over Prime Field and Its Survey,” IJHIT, vol. 7, no. 1, pp. 137–146, Jan. 2014, doi: 10.14257/ijhit.2014.7.1.11.

[90] S. Liu, Q. Mi, and B. Zhu, “Optical image encryption with multistage and multichannel fractional Fourier-domain filtering,” Optics Letters, vol. 26, no. 16, pp. 1242–1244, 2001.

[91] A. A. Abd El-Latif, L. Li, N. Wang, Q. Li, and X. Niu, “A new image encryption based on chaotic systems and singular value decomposition,” in Fourth International Conference on Digital Image Processing (ICDIP 2012), 2012, vol. 8334, pp. 667–671.

[92] M. R. Abuturab, “Color information verification system based on singular value decomposition in gyrator transform domains,” Optics and Lasers in Engineering, vol. 57, pp. 13–19, 2014.

[93] C. Zhang, J. Wang, and X. Wang, “Digital image watermarking algorithm with double encryption by Arnold transform and logistic,” in 2008 Fourth International Conference on Networked Computing and Advanced Information Management, 2008, vol. 1, pp. 329–334.

[94] R. Safabakhsh, S. Zaboli, and A. Tabibiazar, “Digital watermarking on still images using wavelet transform,” in International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004., 2004, vol. 1, pp. 671–675.

[95] M. Arora and M. Khurana, “Secure image encryption technique based on jigsaw transform and chaotic scrambling using digital image watermarking,” Optical and Quantum Electronics, vol. 52, no. 2, pp. 1–30, 2020.

[96] Y. He and Y. Hu, “A proposed digital image watermarking based on DWT-DCT-SVD,” in 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2018, pp. 1214–1218.

[97] P. Khare and V. K. Srivastava, “A secured and robust medical image watermarking approach for protecting integrity of medical images,” Trans. Emerging Tel. Tech., Mar. 2020, doi: 10.1002/ett.3918.

[98] C. Sharma, A. Bagga, B. K. Singh, and M. Shabaz, “A novel optimized graph-based transform watermarking technique to address security issues in real-time application,” Mathematical Problems in Engineering, vol. 2021, 2021.

[99] C. Sharma, A. Bagga, R. Sobti, M. Shabaz, and R. Amin, “A robust image encrypted watermarking technique for neurodegenerative disorder diagnosis and its applications,” Computational and Mathematical Methods in Medicine, vol. 2021, 2021.

[100] C. Agarwal, A. Mishra, and A. Sharma, “A novel gray-scale image watermarking using hybrid Fuzzy-BPN architecture,” Egyptian informatics journal, vol. 16, no. 1, pp. 83–102, 2015.

[101] J. O. Grabbe, “The DES algorithm illustrated,” 2010.

[102] G. Singh, “A study of encryption algorithms (RSA, DES, 3DES and AES) for information security,” International Journal of Computer Applications, vol. 67, no. 19, 2013.

[103] S. Fu-Yan, L. Shu-Tang, and L. Zong-Wang, “Image encryption using high-dimension chaotic system,” Chinese Physics, vol. 16, no. 12, p. 3616, 2007.

[104] X.-Y. Wang and Z.-M. Li, “A color image encryption algorithm based on Hopfield chaotic neural network,” Opt. Lasers Eng., vol. 115, pp. 107–118, Apr. 2019, doi: 10.1016/j.optlaseng.2018.11.010.

[105] M. Khan, “A novel image encryption scheme based on multiple chaotic S-boxes,” Nonlinear Dyn., vol. 82, no. 1–2, pp. 527–533, Oct. 2015, doi: 10.1007/s11071-015-2173-3.

[106] M. Khan and T. Shah, “An efficient chaotic image encryption scheme,” Neural Comput & Applic, vol. 26, no. 5, pp. 1137–1148, Jul. 2015, doi: 10.1007/s00521-014-1800-0.

[107] F. Amounas and E. H. El Kinani, “Fast mapping method based on matrix approach for elliptic curve cryptography,” International Journal of Information & Network Security (IJINS), vol. 1, no. 2, pp. 54–59, 2012.

[108] P. Bh, D. Chandravathi, P. P. Roja, and Others, “Encoding and decoding of a message in the implementation of Elliptic Curve cryptography using Koblitzs method,” International Journal on Computer Science and Engineering, vol. 2, no. 5, pp. 1904–1907, 2010.

[109] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, “An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing,” Information Sciences, vol. 556, pp. 305–340, 2021.

[110] X. Chai, Y. Chen, and L. Broyde, “A novel chaos-based image encryption algorithm using DNA sequence operations,” Opt. Lasers Eng., vol. 88, pp. 197–213, Jan. 2017, doi: 10.1016/j.optlaseng.2016.08.009.

[111] K. A. K. Patro, B. Acharya, and V. Nath, “Secure, Lossless, and Noise-resistive Image Encryption using Chaos, Hyper-chaos, and DNA Sequence Operation,” IETE Technical Review, pp. 1–23, Apr. 2019, doi: 10.1080/02564602.2019.1595751.

[112] R. E. Boriga, A. C. Dascalescu, and A. V. Diaconu, “A new fast image encryption scheme based on 2D chaotic maps,” IAENG International Journal of Computer Science, vol. 41, no. 4, pp. 249–258, 2014.

[113] Y. Zhang and D. Xiao, “An image encryption scheme based on rotation matrix bit-level permutation and block diffusion,” Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 1, pp. 74–82, 2014.

[114] A. Belazi, A. A. Abd El-Latif, and S. Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos,” Signal Processing, vol. 128, pp. 155–170, Nov. 2016, doi: 10.1016/j.sigpro.2016.03.021.

[115] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, “A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps,” 3D Res., vol. 7, no. 1, p. 7, Mar. 2016, doi: 10.1007/s13319-016-0084-9.

[116] Y. Xian and X. Wang, “Fractal sorting matrix and its application on chaotic image encryption,” Information Sciences, vol. 547, pp. 1154–1169, 2021.

[117] K. A. Kumar Patro and B. Acharya, “An efficient colour image encryption scheme based on 1-D chaotic maps,” Journal of Information Security and Applications, vol. 46, pp. 23–41, Jun. 2019, doi: 10.1016/j.jisa.2019.02.006.

[118] K. A. K. Patro and B. Acharya, “A novel multi-dimensional multiple image encryption technique,” Multimedia Tools and Applications, vol. 79, no. 19, pp. 12959–12994, 2020.

[119] Q. Lu, C. Zhu, and X. Deng, “An efficient image encryption scheme based on the LSS chaotic map and single S-box,” IEEE Access, vol. 8, pp. 25664–25678, 2020.

[120] L. Liu, Y. Lei, and D. Wang, “A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation,” IEEE access, vol. 8, pp. 27361–27374, 2020.

[121] J. S. Khan et al., “DNA and plaintext dependent chaotic visual selective image encryption,” IEEE Access, vol. 8, pp. 159732–159744, 2020.

Turnitin Originality Report

Efficient Design of Cryptographic Scheme Based on Elliptic Curve Cryptography for Multimedia Data Security by Ijaz Khalid

From PhD (PhD DRSML)

turnitin

- Processed on 31-Aug-2023 08:16 PKT
- ID: 2154707633
- Word Count: 30518

Similarity Index
14%
Similarity by Source

Internet Sources:
9%
Publications:
9%
Student Papers:
2%

sources:

1 1% match (Internet from 18-Apr-2023)

https://www.researchgate.net/publication/344293359_An_efficient_image_encryption_scheme_for_TMIS_based_on_elliptic_curve_integrated_

2 1% match ()

Asif, Raqib Ahmed. "Efficient Computation For Hyper Elliptic Curve Based Cryptography", 'University of Windsor Leddy Library', 2016

3 1% match ("Guide to Elliptic Curve Cryptography", Springer Nature, 2004)

"Guide to Elliptic Curve Cryptography", Springer Nature, 2004

4 < 1% match (Internet from 23-Feb-2023)

https://www.researchgate.net/publication/262191712_A_symmetric_image_encryption_algorithm_based_on_mixed_linear-nonlinear_coupled_map_lattice

5 < 1% match (Internet from 23-Sep-2022)

https://www.researchgate.net/publication/277725688_An_efficient_chaotic_image_encryption_scheme

6 < 1% match (Internet from 25-Feb-2023)

https://www.researchgate.net/publication/293329501_A_new_RGB_image_encryption_algorithm_based_on_DNA_encoding_and_elliptic_curv
Hellman_cryptography

7 < 1% match (Internet from 28-Jan-2023)

https://www.researchgate.net/publication/306071902_A_Novel_Approach_for_Speech_Encryption_Zaslavsky_Map_as_Pseudo_Random_Nun

8 < 1% match (Internet from 30-Jan-2023)

https://www.researchgate.net/publication/272555992_An_efficient_chaotic_image_encryption_based_on_alternate_circular_S-boxes

9 < 1% match (Internet from 28-Jan-2023)

https://www.researchgate.net/publication/282495454_Audio_encryption_based_on_the_cosine_number_transform

10 < 1% match (Internet from 30-Jan-2023)

https://www.researchgate.net/publication/301273723_A_fast_image_encryption_algorithm_based_on_chaotic_map

11 < 1% match (Internet from 24-Feb-2023)

https://www.researchgate.net/publication/257553371_An_Image_Encryption_Scheme_Based_on_Elliptic_Curve_and_a_Novel_Mapping_Meth

12 < 1% match (Internet from 03-Feb-2023)