

**A novel color image encryption scheme based on a new dynamic
compound chaotic map and S-box**

A PROJECT REPORT

Submitted by

112818104044

M.Praveen Kumar

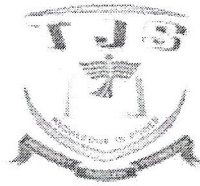
112818104021

V.Jeeva

112818104009

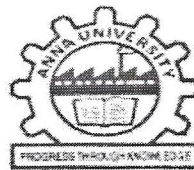
K.Bharathi Raja

in partial fulfillment for the award of the degree
of
BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE AND ENGINEERING




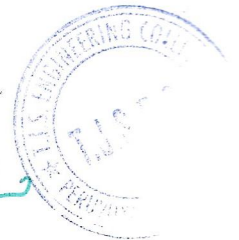
T.J.S ENGINEERING COLLEGE
PERUVOYAL (NEAR KAVARAIPETTAI)
GUMMIDIPOONDI TALUK
THIRUVALLUR DISTRICT – 601206

Approved by AICTE and Affiliated to Anna University, Chennai



ANNA UNIVERSITY::CHENNAI 600 025


PRINCIPAL
T.J.S. ENGINEERING COLLEGE
Peruvoyal, Kavaraipettai,
Gummidipoondi Taluk,
Thiruvallur Dist - 601 206.



ANNA UNIVERSITY : CHENNAI 600025

BONAFIDE CERTIFICATE

Certified that this project report "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box" is the bonafide work of the following students

112818104044

M.Praveen Kumar

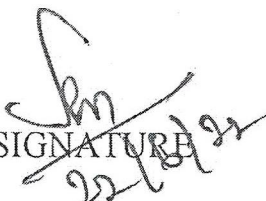
112818104021

V.Jeeva

112818104009

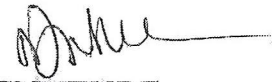
K.Bharathi Raja

who carried out the project work under my supervision.


SIGNATURE
22/6/22

Mr.Senthil Kumar
SUPERVISOR

DEPARTMENT OF COMPUTER SCIENCE
AND ENGINEERING
T.J.S. ENGINEERING COLLEGE



SIGNATURE

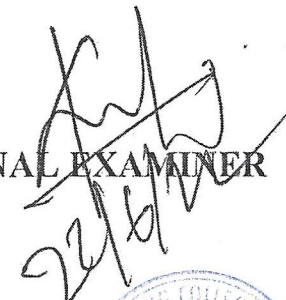
Department of CSE
T.J.S. Engineering College
Peruvoyal, Kaveraipeetai,
Thiruvallur Dist - 601 206.

Dr.S.Anbu,M.E.,Ph.D.,
HEAD OF THE DEPARTMENT
DEPARTMENT OF COMPUTER SCIENCE
AND ENGINEERING
T.J.S. ENGINEERING COLLEGE

Submitted for the viva voce examination held on 22/6/2022. at T.J.S Engineering College, Peruvoyal.


INTERNAL EXAMINER


PRINCIPAL
T.J.S. ENGINEERING COLLEGE
Peruvoyal, Kaveraipeetai,
Gummidipoondi Taluk,
Thiruvallur Dist - 601 206.


EXTERNAL EXAMINER
22/6/22



Abstract

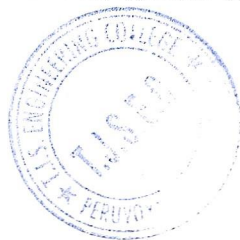
Data security is the science of protecting data in information technology, including authentication, data encryption, data decryption, data recovery, and user protection. To protect data from unauthorized disclosure and modification, a secure algorithm should be used. Many techniques have been proposed to encrypt text to an image. Most past studies used RGB layers to encrypt text to an image. In this paper, a Text-to-Image Encryption-Decryption algorithm is proposed to improve security, capacity, and processing time. Digital image encryption is widely used for secure image transmission over the internet.

Therefore, this thesis provides a brief background and discussion about digital image encryption, analyzing existing literature on different digital image encryption algorithms. Moreover, a three-layer image encryption scheme for digital art using logistic map, S-box and Tan logistic map is proposed in this paper. Subsequently, the proposed scheme is evaluated by conducting multiple performance metrics, which resulted in a good performance when compared to the literature.

The method therefore simultaneously owns both image encryption and lossless compression abilities. The given image is first partitioned into non-overlapping fixed-size sub images, and each sub image will then have its own base value. These sub images are then encoded and encrypted one by one according to the base values. By choosing the function to encrypt the base value, there are $(128!)^t$ (or $(128!)^{3t}$) possible ways to encrypt a gray-scaled (color) image if t layers are used in the encryption system. The theoretical analysis needed to build up the proposed encryption method is provided, and the experimental results are also presented.

In modern technological era image encryption has become an attractive and interesting field for researchers. They work for improving the security of image data from unauthorized sources. Chaos theory, due to its randomness and unpredictable behaviors, is considered favorite for the purpose of image encryption.

This paper proposes a diffusion based image encryption algorithm by using chaotic maps. Firstly a chaotic map (piecewise linear chaotic map) is used for the generation of S-box, then it is used for the pixel values modification to generate element of non-linearity. After this these modified values are further diffused with another random sequence, generated by tent logistic chaoticmap.



PRINCIPAL
T.J.S. ENGINEERING COLLEGE
Peruvoyal, Kavaraipettai,
Gummidipondi Taluk,
Thiruvallur Dist - 601 206.

OBJECTIVES:

- To understand Cryptography Theories, Algorithms and Systems.
- To understand necessary Approaches and Techniques to build protection mechanisms in order to secure computer networks.

UNIT I INTRODUCTION**9**

Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis.

UNIT II SYMMETRIC KEY CRYPTOGRAPHY**9**

MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures - Modular arithmetic- Euclid's algorithm- Congruence and matrices - Groups, Rings, Fields- Finite fields- SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES – Differential and linear cryptanalysis - Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Advanced Encryption Standard - RC4 – Key distribution.

UNIT III PUBLIC KEY CRYPTOGRAPHY**9**

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing –Factorization – Euler's totient function, Fermat's and Euler's Theorem - Chinese Remainder Theorem – Exponentiation and logarithm - ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange - ElGamal cryptosystem – Elliptic curve arithmetic-Elliptic curve cryptography.

UNIT IV MESSAGE AUTHENTICATION AND INTEGRITY**9**

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – SHA – Digital signature and authentication protocols – DSS- Entity Authentication: Biometrics, Passwords, Challenge Response protocols- Authentication applications - Kerberos, X.509

UNIT V SECURITY PRACTICE AND SYSTEM SECURITY**9**

Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.

TOTAL 45 PERIODS**OUTCOMES:****At the end of the course, the student should be able to:**

- Understand the fundamentals of networks security, security architecture, threats and vulnerabilities
- Apply the different cryptographic operations of symmetric cryptographic algorithms
- Apply the different cryptographic operations of public key cryptography
- Apply the various Authentication schemes to simulate different applications.
- Understand various Security practices and System security standards

TEXT BOOK:

1. William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

REFERENCES:

1. C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wiley India Pvt.Ltd
2. Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw Hill 2007.


PRINCIPAL
T.J.S. ENGINEERING COLLEGE
 Peruvoyal, Kavaraipettai,
 Gummidipoondi Taluk,
 Thiruvallur Dist - 601 206.

