VISVESVARAYA TECHNOLOGICAL UNIVERSITY
Jnana Sangama, Belagavi-590018, Karnataka

Project Synopsis

on

DESIGN AND ANALYSIS OF CRYPTOGRAPHIC TECHNIQUE FOR IMAGE ENCRYPTION

Submitted by

USN	Student Name
1BG19EC092	Sanjan Raj S
1BG19EC112	Surya Kaushik P K
1BG19EC122	Vikas P

Batch No: B9

Vidyayāmruthamashnuthe

B.N.M. Institute of Technology

An Autonomous Institution under VTU, Approved by AICTE, Accredited as ‘A’ Grade Institution by NAAC till 31.12.2026
All Eligible UG branches – CSE, ECE, EEE, ISE & Mech.Engg. Accredited by NBA till 30.06.2025
Post box no. 7087, 27th cross, 12th Main, Banashankari 2nd Stage, Bengaluru- 560070, INDIA
Ph: 91-80- 26711780/81/82 Email: principal@bnmit.in, www.bnmit.org

Department of Electronics & Communication Engineering

2022-2023

Batch Number	B9
Project Title:	Design and Analysis Of Cryptographic Technique For Image Encryption
Place where project is being carried out:	BNM Institute of Technology
External Guide: Contact Details:	-
Name and signature of the Internal guide:	PRIYA SANKPAL
Date of submission:	

USN	Name	Contact Number	Email Id	Signature
1BG19EC092	Sanjan Raj S	9019646281	sanjanrajs96@gmail.com	
1BG19EC112	Surya Kaushik P K	9845658876	pskaushik007@gmail.com	
1BG19EC122	Vikas P	8088054253	vikasvikas41903@gmail.com	

Project Coordinator **HoD, ECE**

CONTENTS

1. INTRODUCTION

Computer technology needed in human life. Almost every man needs computer assistance in their daily lives. Each person will have an important document that is confidential which can only be accessed by certain people. The problem of computer security is something crucial in this information age. There are several techniques for data security one of which is a disguise or cryptographic techniques. Cryptography is the art and science to protect the data by transforming it into a specific code and is intended only for people who have the key to change the code back to normal. In the field of cryptography, there are three crucial concepts that encryption, decryption, and key. Encryption is the process of transforming information (plain text) into a code that is not recognizable (cipher text) by using a key. Decryption is the process of converting code that is not identifiable (cipher text) into information (plain text) using a key, in this case, the encrypted files in text files. To implement encryption and decryption, it needs an appropriate encryption and decryption algorithm[4]. In this paper, Vigenere cipher will be used for image encryption and decryption. Vigenere cipher is a classic cryptography implemented symmetric keys. It is a poly-alphabetic substitution that works based on Caesar cipher implementing Vigenere Square. In this digital world, an image is a collection of the pixel which has different intensity values. Each image consists of n*m number of pixel, where n is the number of rows and m is the number of columns. A pixel (picture element) is a small block that represents the amount of gray intensity to be displayed for that particular portion of the image. For most images, pixel values are integers that range from 0 (black) to 255 (white). An RGB image or a true color image is an image in which each pixel has three components. These components are red (R), green (G) and blue (B), so that the RGB image are m-by-n-by-3 array of class uint8, uint16, single, or double whose pixel values specify intensity values. The multiple values may correspond to different color intensities.

2. MOTIVATION

Nowadays, aspect of security of information is above all aspects. Care is to be taken to maintain the confidentiality of information. Encryption algorithms are used to turn plain image to cipher image. Cipher image in every way should be different from original image. Image encryption technique is categorized by following aspects:

- Pixel position permutation aspect
- Value transformation aspect
- Visual transformation aspect

If any algorithm is made keeping in mind all above three aspects, then a good algorithm can be developed. Cryptographies secret information is sent from one side to another over insecure communication channel. Cryptography is used in fields like military imaging, military communication, telemedicine, banking, multimedia systems, and internet communication.

3. OBJECTIVE AND SCOPE

Cryptography is a method of securing text data, images and sound in order to secure its confidentiality and to minimize data stealing, attack, etc. The scope is to improve classic Vigenere cipher and polybius cipher on image encryption. This project uses both RGB and grayscale images as samples and shows that Vigenere cipher and polybius cipher has better performance in encrypting an image both visually and its randomness.

The objectives of the project are to:

- Transfer the image securely
- Encrypt & Decrypt the image using vigenere and polybius cipher

4. DESCRIPTION OF PROJECT

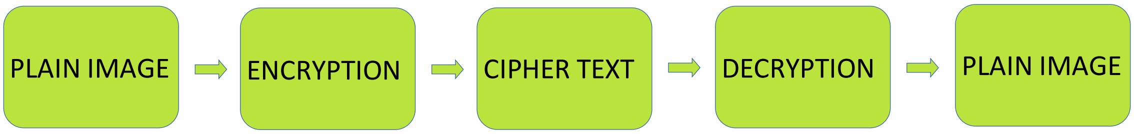
4.1 HARDWARE REQUIREMENTS:

- Laptop or PC, windows 7 or higher

4.2 SOFTWARE REQUIREMENTS:

- Python

4.3 BLOCK DIAGRAM:



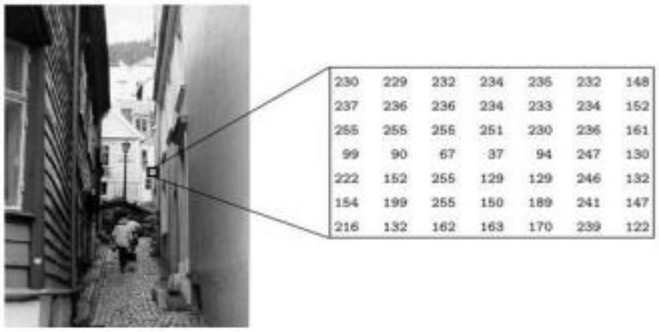
4.4 WORKING:

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions. In Substitution Cipher Technique plain image characters are replaced with other characters, numbers and symbols as well as in substitution Cipher Technique, character's identity is changed while its position remains unchanged. Example – Polybius Cipher, Vigenère Cipher.

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table. This makes the cipher less vulnerable to cryptanalysis using letter frequencies. Blaise de Vigenère developed what is now called the Vigenère cipher in 1585. He used a table known as the Vigenère square, to encipher messages, images.

Encryption: Ci = (Pi + Ki) mod 256

Decryption: Pi¬ = (Ci + Ki) mod 256



230	229	232	234	235	232	148
237	236	236	234	233	234	152
255	255	255	251	230	236	161
99	90	67	37	94	247	130
222	152	255	129	129	246	132
154	199	255	150	189	241	147
216	132	162	163	170	239	122

Gray-scale Image 8bit

A Polybius Square is a table that allows someone to convert letters into numbers. To make the encryption little harder, this table can be randomized and shared with the recipient. In order to fit the 26 letters of the alphabet into the 25 cells created by the table, the letters ‘i’ and ‘j’ are usually combined into a single cell. Originally there was no such problem because the ancient greek alphabet has 24 letters. A table of bigger size could be used if a language contains large number of alphabets.

5. CONCLUSION

Cryptography is generally utilized technique for the security of data. Vigenère cipher is one of the cryptographic techniques that are viewed as least complex and most vulnerable because of numerous impediments. To conquer the impediments of Vigenere cipher we proposed an upgraded variant as Combination of Polybius cipher that is a lot of secure against Kasiski and Friedman assaults. Cryptanalysis, frequency analysis, pattern prediction and brute attack on proposed technique are also much difficult due to use of multiples tables for encryption.

REFERENCES

[1] International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV6IS010223 (This work is licensed under a Creative Commons Attribution 4.0 International License.) Published by : Vol. 6 Issue 01, January-2017 http://www.ijert.org. (

[2] International Journal of Engineering & Technology, 7 (2.2) (2018) 62-64 International Journal of Engineering & Technology Website: www.sciencepubco.com/index.php/IJET.

[3] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 5, May 2013).

[4] International Journal of Pure and Applied Mathematics Volume 118 No. 24 2018 ISSN: 1314-3395 (on-line version) url: http://www.acadpubl.eu/hub/