

Encrypting & Decrypting Images

Using the Feistel Network (Cipher)

 FACULTY OF INFORMATION TECHNOLOGY

 SUPERVISING LECTURER

Prof. Mohammed M Abu Shquier

 PARTICIPATING STUDENTS

230676 Ali Ahmad Mohammed Eid Eid

220647 Husam Ahmad Mahmoud Eid

231235 Emad Addin Hikmat Jamal Zureigat

 Spring 2026

 Graduation Project (1) - 1004482



SECURITY-FOCUSED GOALS

Project Goals

The Feistel cipher algorithm provides comprehensive protection for encrypted images



01

Confidentiality

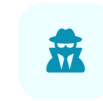
Prevent unauthorized access to encrypted image content



02

Data Protection

Secure sensitive images (personal, medical, financial) from leaks



03

Privacy Preservation

Ensure images cannot be viewed without the correct key



04

Secure Storage & Transfer

Protect images when stored locally or sent over networks



05

Demonstrate Cryptography Concepts

Show how block ciphers can secure real-world data



06

Mitigate Simple Attacks

Make raw file inspection or basic data recovery ineffective

Role of Feistel in Image Cryptography

How Feistel networks contribute to modern encryption systems



01

Foundation of Real Ciphers

Used in DES, GOST, Blowfish, and Two-fish algorithms. Influenced modern encryption designs.



02

Reversibility

Encryption and decryption use the same structure. Efficient for image data processing.



03

Block-Based Processing

Fits naturally with image files, which are handled as blocks of bytes.



04

Security Principles

Demonstrates confusion and diffusion—essential concepts for protecting image data.



05

Educational Value

Helps understand how modern ciphers like AES achieve strong security.



06

Implementation Efficiency

Round function can be arbitrarily complex without requiring invertibility.

Image Architecture RGB

Understanding how colors are represented in digital systems



Red

8 bits per channel, $2^8 = 256$ values (0-255)



Green

Same structure 8 bits, 256 intensity levels



Blue

24-bit color total (8 × 3 channels)

Red Pixel

R=255, G=0, B=0

Red: **11111111**

Green: **00000000**

Blue: **00000000**

16.7M

Possible Colors

256×256×256

Total Colors

The Feistel Cipher

A symmetric structure for building block ciphers - foundation of modern encryption

Definition

A Feistel cipher (or Luby-Rackoff block cipher) is a **symmetric structure** used in constructing block ciphers. Named after **Horst Feistel**, the German-born physicist and cryptographer who pioneered research at IBM.

Algorithms Using It

US DES

Soviet/Russian GOST

Blowfish

Two-fish



Invertible Operation

Entire operation is guaranteed to be invertible even if the round function is not itself invertible



Implementation Efficiency

Round function can be made arbitrarily complex since it doesn't need to be designed for invertibility



Encryption/Decryption Similarity

Both operations are very similar, requiring only a reversal of the key schedule



No S-Box Dependency

Doesn't depend on substitution boxes that could cause timing side-