# ENHANCING DATA SECURITY USING DIGITAL WATERMARKING

**By**
Nayan S. Thorat (66)
Prathamesh A. Yelne (74)
Zibal A. Khan (30)
Om V. Ubhad (70)
Shraddha V. Jaiswal (25)

**Guide**
Mr. Chetan R. Ingole

**Department of Computer Science and Engineering**
Prof Ram Meghe College of Engineering and Management
Badnera-Amravati, India.

2022-2023

# Content

- Introduction
- Origin of Name “Digital Watermarking”
- Objective of this Project
- Literature Analysis
- Algorithms
- Technology and Platform to be used
- AFD, DFD and CFD
- Application of Digital Watermarking
- Conclusion
- Demonstrate of this project (Optional)
- References

# Introduction

**Digital Watermark** is a mark or, in many cases, a piece of code embedded into digital data (videos, pictures, or even audio). Digital watermarks, also known as **forensic watermarks.** Digital watermarks protect the piece of digital media and prevent copyright infringement.

# Origin of Name "Digital Watermarking"

The term "**Digital Watermark**" was coined by **Andrew Tirkel** and **Charles Osborne** in **December 1992.** The first watermarks appeared in **Italy** during the **13th century**, but their use rapidly spread across **Europe.**

**Andrew Tirkel**

**Charles Osborne**

# Objective of this Project

i) To prevents data leakage

ii) To protects copyright of multimedia data

iii) To protects databases and text files.

iv) To provide secret communication between one organization to other organization

v) To hide a message related to the actual content in the form of digital signal (Morse Code)

# Literature Analysis

| Reference | Basic concept | Database | Keywords | Claim by Authors |
|---|---|---|---|---|
| **[1] Jaishri Huru, Hemant Damecha (2014)** | **Watermarking Algorithms for Digital Image** | **Embedded Data** | **Reduction of image size, lossy compression of image,<br>changing the contrast of the images** | **Watermarking are diverse and classified based on their visibility and robustness** |
| **[2] Mohan Durvey (2014)** | **Digital Watermarking** | **Embedded Data** | **Types of watermarks, Spatial watermarking, Frequency domain watermarking and<br>Applications of watermarking** | **Protecting the digital media from unauthorized usage** |
| [3] Abraham and Paul (2019) | An imperceptible spatial domain color image watermarking scheme | Embedded Data | Color image watermarking, Spatial domain, Watermark, Embedding, Extraction, Attacks | Watermark information over a region of pixels as implemented by the transform domain techniques. |

# Literature Analysis

| Reference | Basic concept | Database | Keywords | Claim by Authors |
|---|---|---|---|---|
| [4] Sarita P. Ambadekar, Jayshree Jain and Jayshree Khanapuri | Digital Image Watermarking Through Encryption and DWT for Copyright Protection | Embedded Data | Image watermarking, Discrete wavelet, transform, Encryption, Copyright protection | Applied for copyright and content authentication applications. |
| [5] Zihan Yuan, Decheng Liu, Xueting Zhang, Qingtang Su (2020) | New image blind watermarking method based on two dimensional discrete cosine transform | Embedded Data | Digital image watermarking, Discrete cosine transform (DCT) | Application of watermarking with 2D |
| [6] I.J, Cox, J.Killian, F.T.Leighton, and T,Shamoon (1997) | Secure spread spectrum watermarking of multimedia | Embedded Data | Digital image watermarking, Image Processing | Spectrum watermarking |

# Algorithms

1) SHA - 256 Algorithm (data integrity)

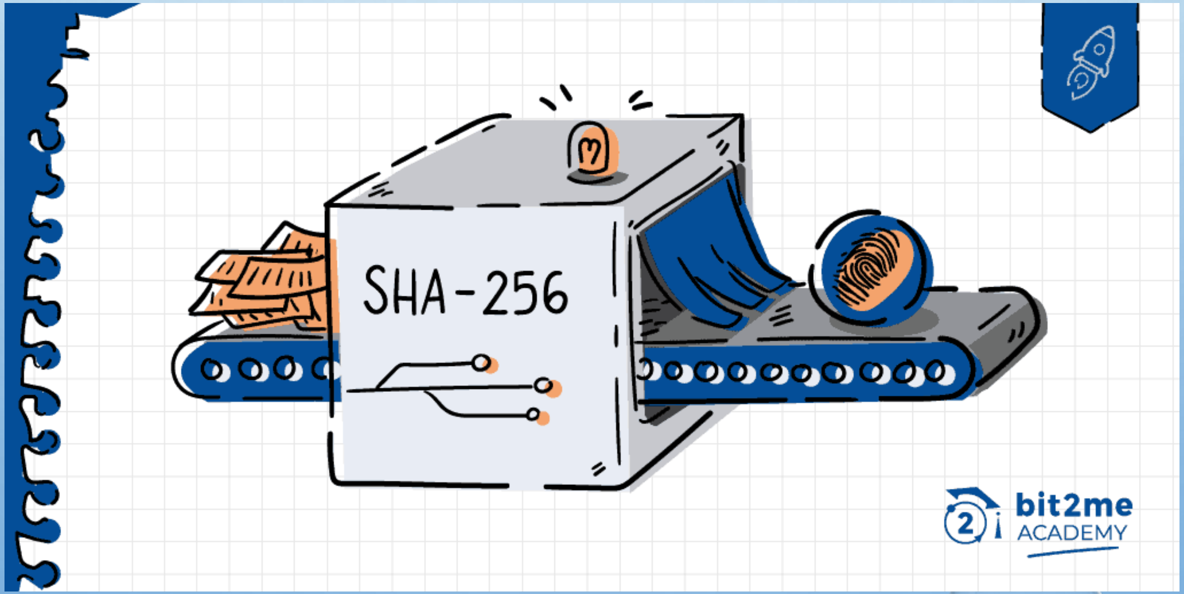
2) AES Algorithm (database)

3) XOR Algorithm (binary operation)

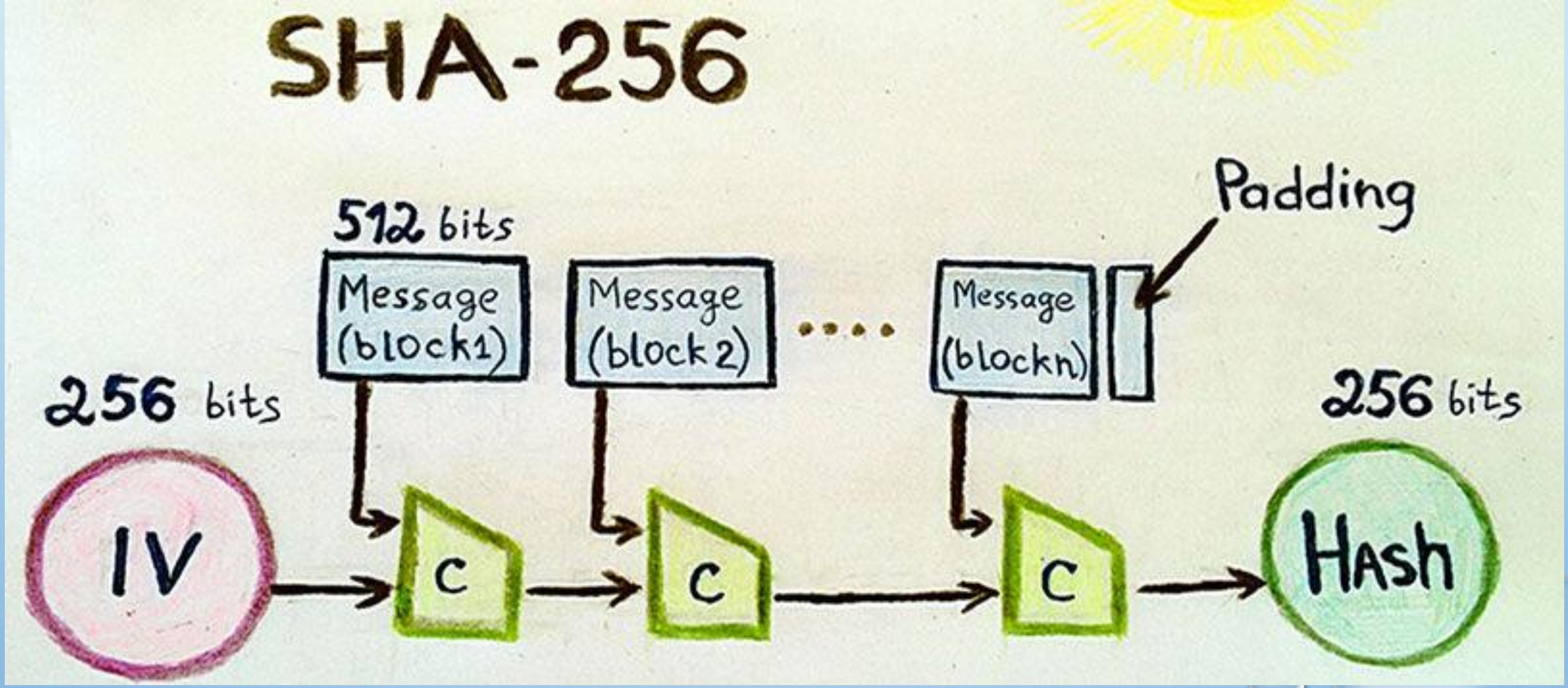
4) RC6 Algorithm (block operation)

# SHA 256 Algorithm

**SHA-256 (Secure Hash Algorithm 256)** is a cryptographic hashing algorithm (or function) that's used for **message, file, and data integrity verification.** It's part of the **SHA-2 family** of **hash functions.**



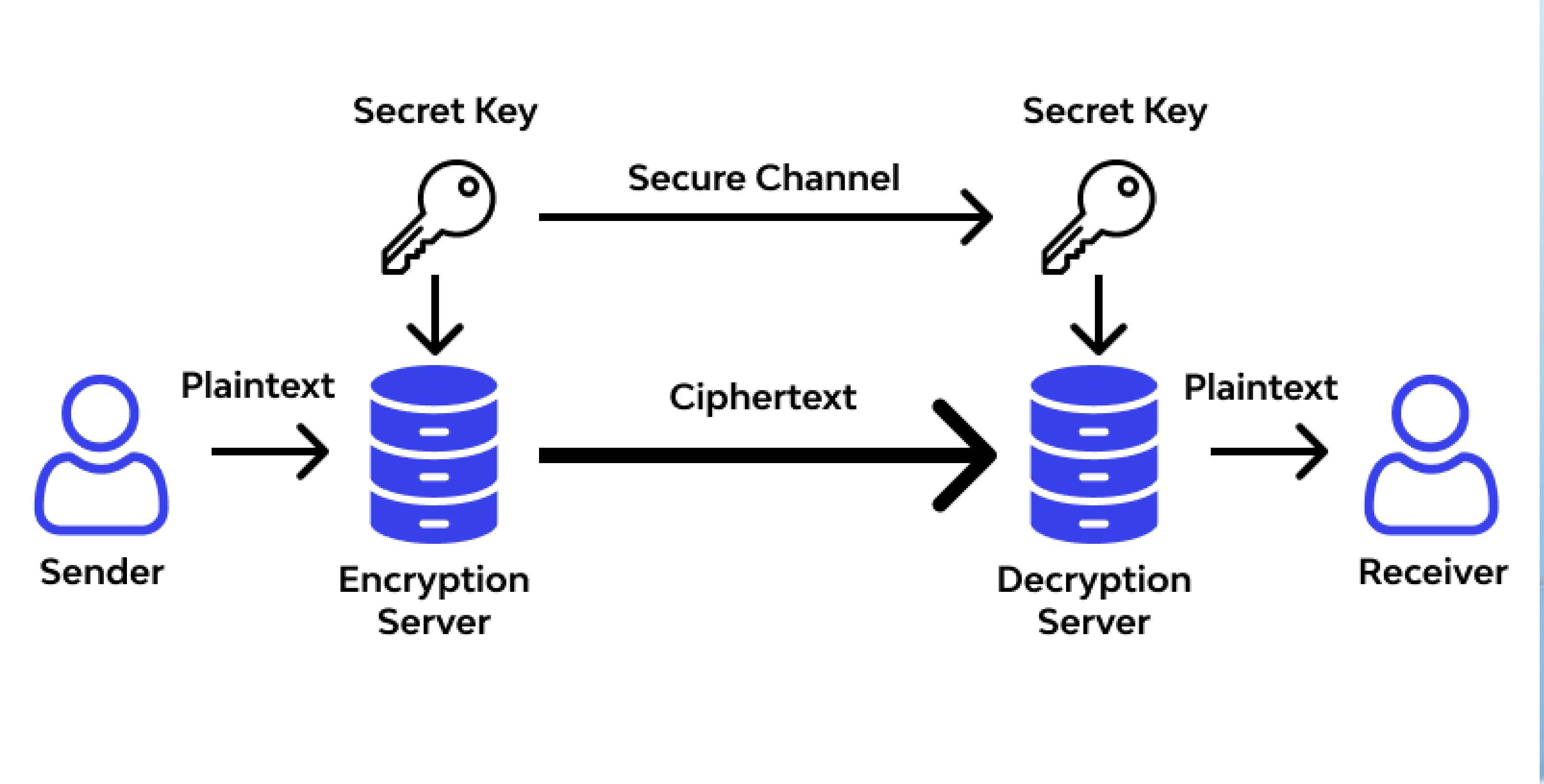
# Working of SHA 256



# AES Algorithm

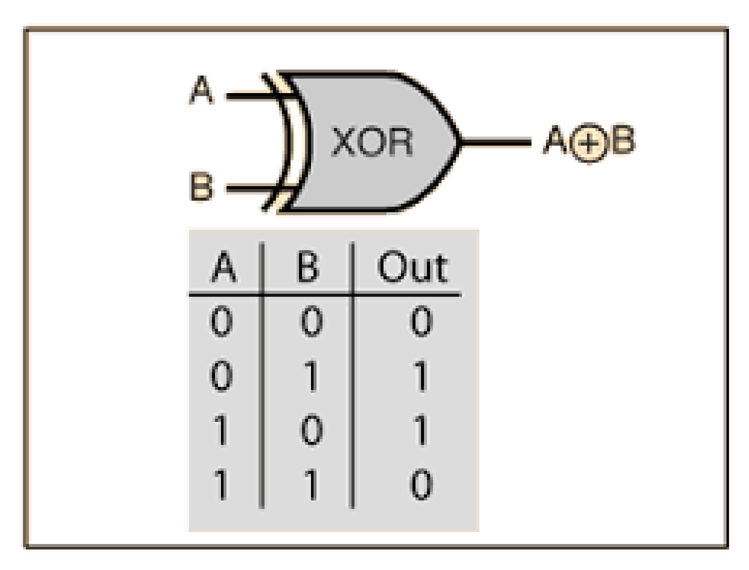
**AES (Advanced Encryption Standard)** is a **symmetric** type of encryption which is used the **same key** for **both encrypt and decrypt data.** It is based on a **substitution-permutation network,** also known as an **SP network**

# Working of AES



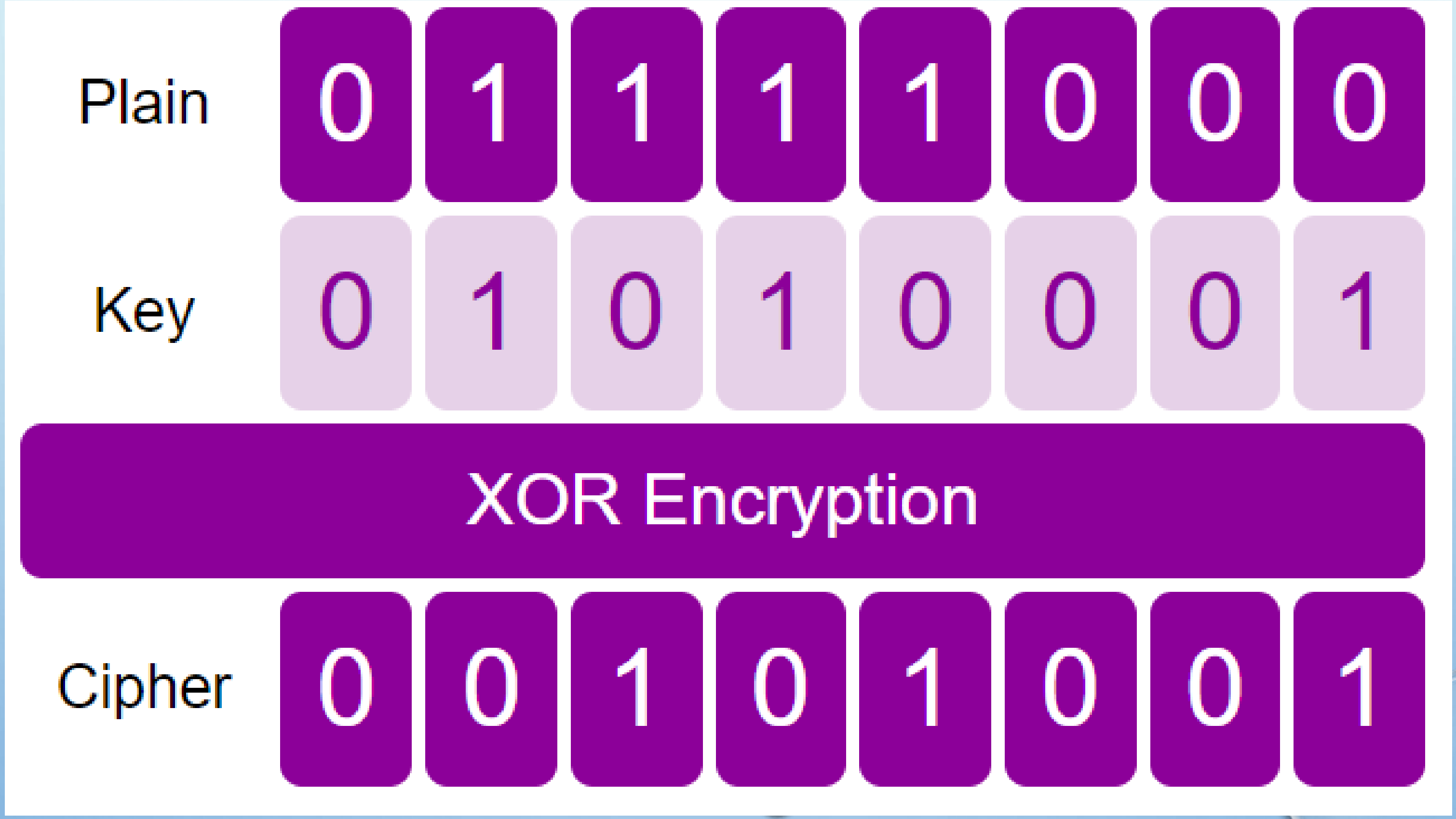
# XOR Algorithm

XOR (Exclusive OR) is a **symmetrical encryption and decryption method** based on the use of the **logical with binary operator.** It is used for **generating parity bits** for **error checking** and **fault tolerance.**



| A | B | Out |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

# Working of XOR



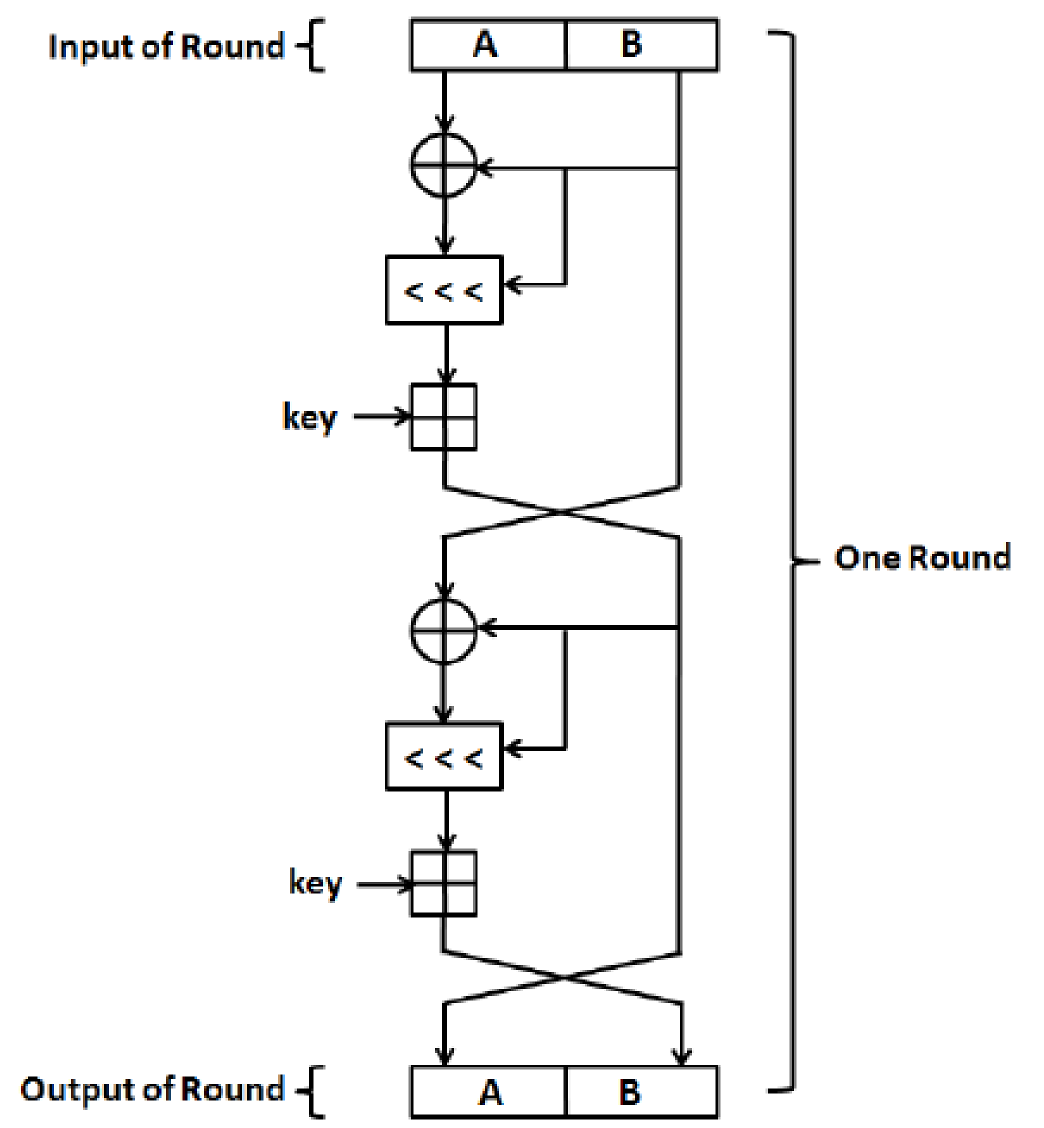
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Plain | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| Key | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| XOR Encryption | | | | | | | | |
| Cipher | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |

# RC6 Algorithm

**RC6 (Rivest Cipher 6)** is a **block encryption and decryption algorithm** based on **RC5 algorithm.** It is a block cipher with **a two-word input (plaintext)** and a **two-word output (ciphertext)** block size.

RC6

# Working of RC6



# Technology and Platform to be used

**Deployment Platform: -** Windows 10 / Windows 11

**Application Server: -** Apache Server

**Software Environment: -** Java 19.0.2 and Python 3.11.2

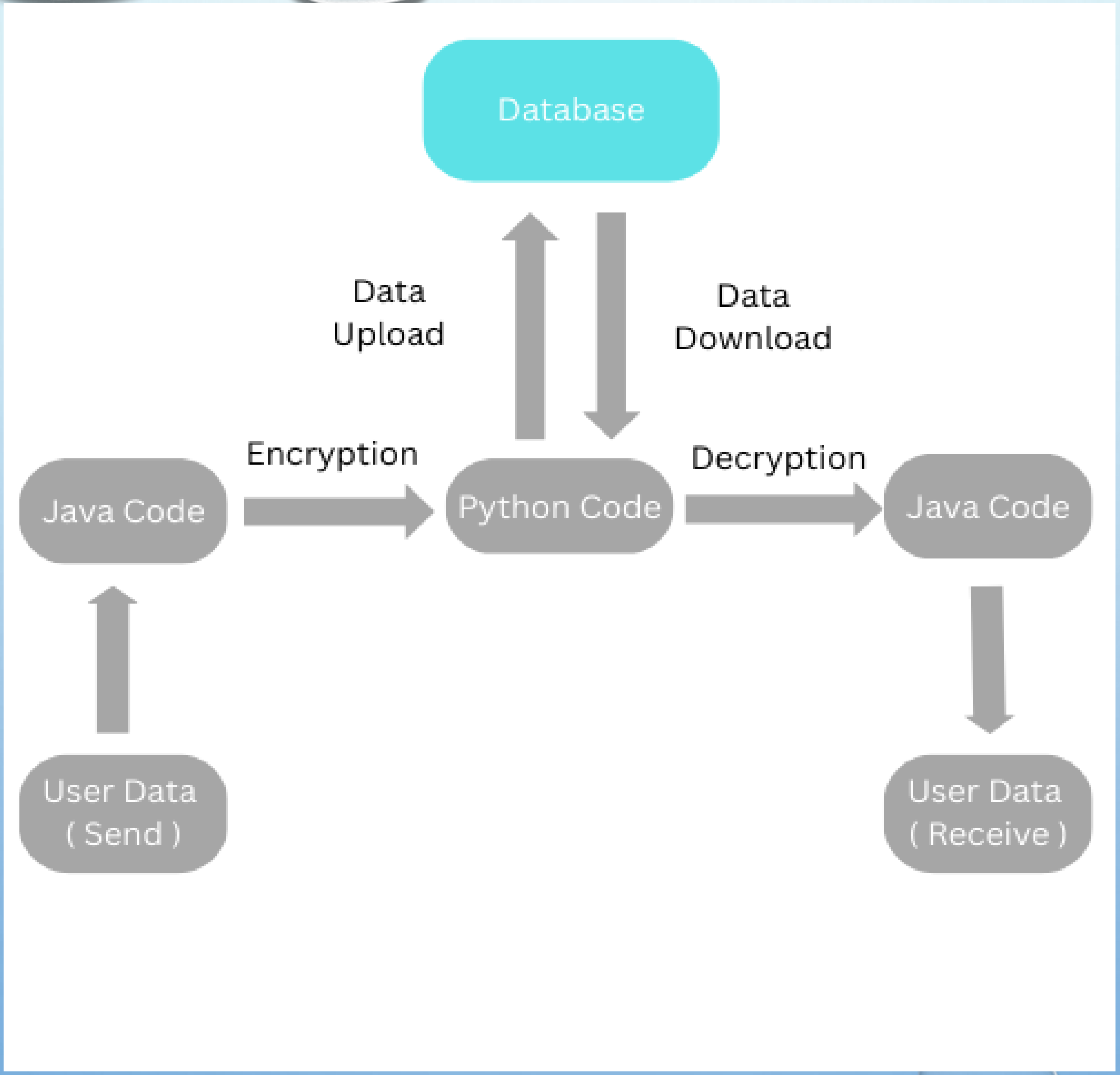
**Framework: -** Springboot 2.5.3

**Database Technologies: -** MySQL Workbench (include MySQL Server, Connector Java, Connector Python, MySQL Shell)

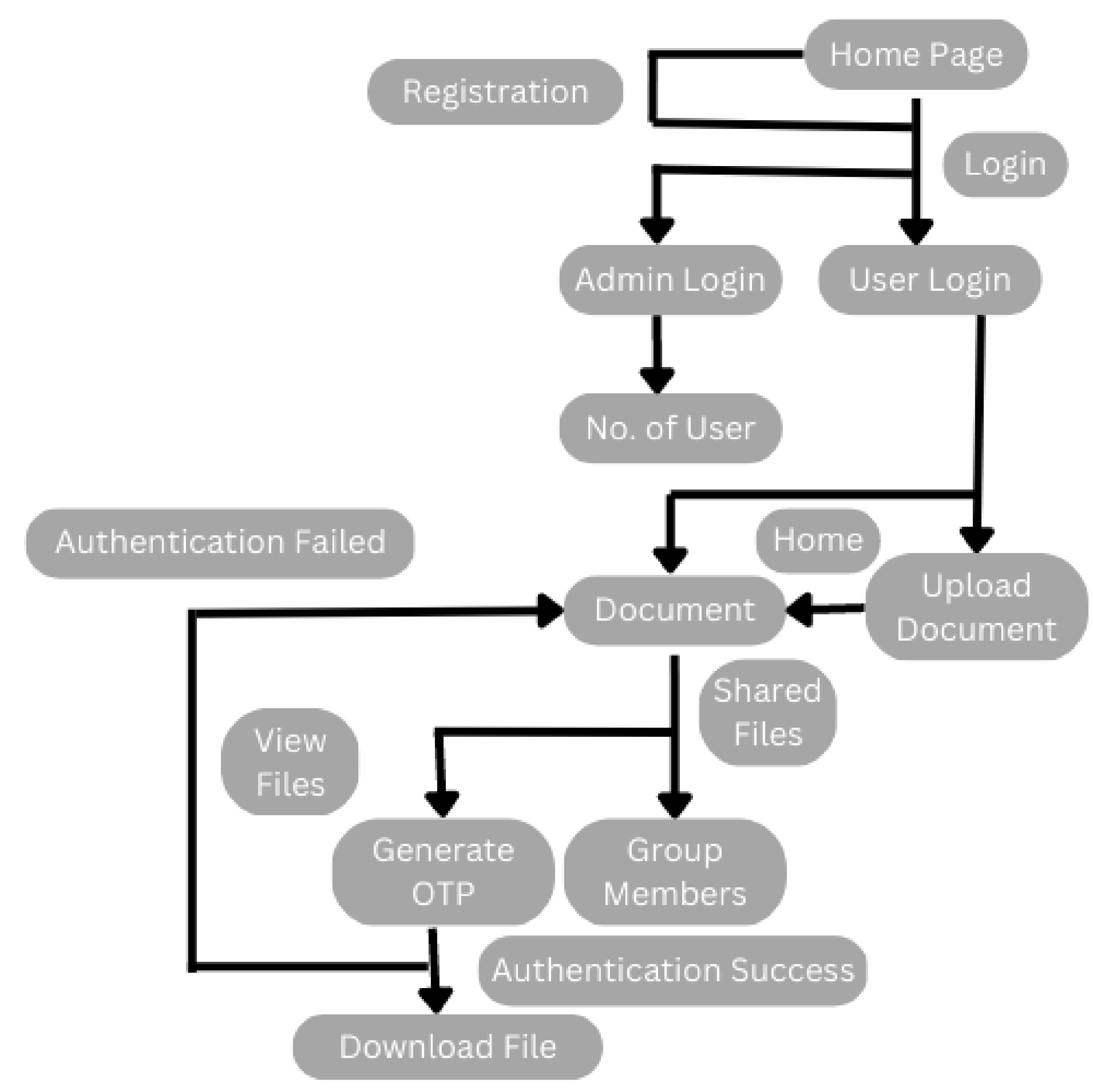
**Web Development : -** HTML5, JavaScript, JSP

**Development Tools: -** Eclipse IDE for Java Developer, Sublime Text and Pycharm Community Edition

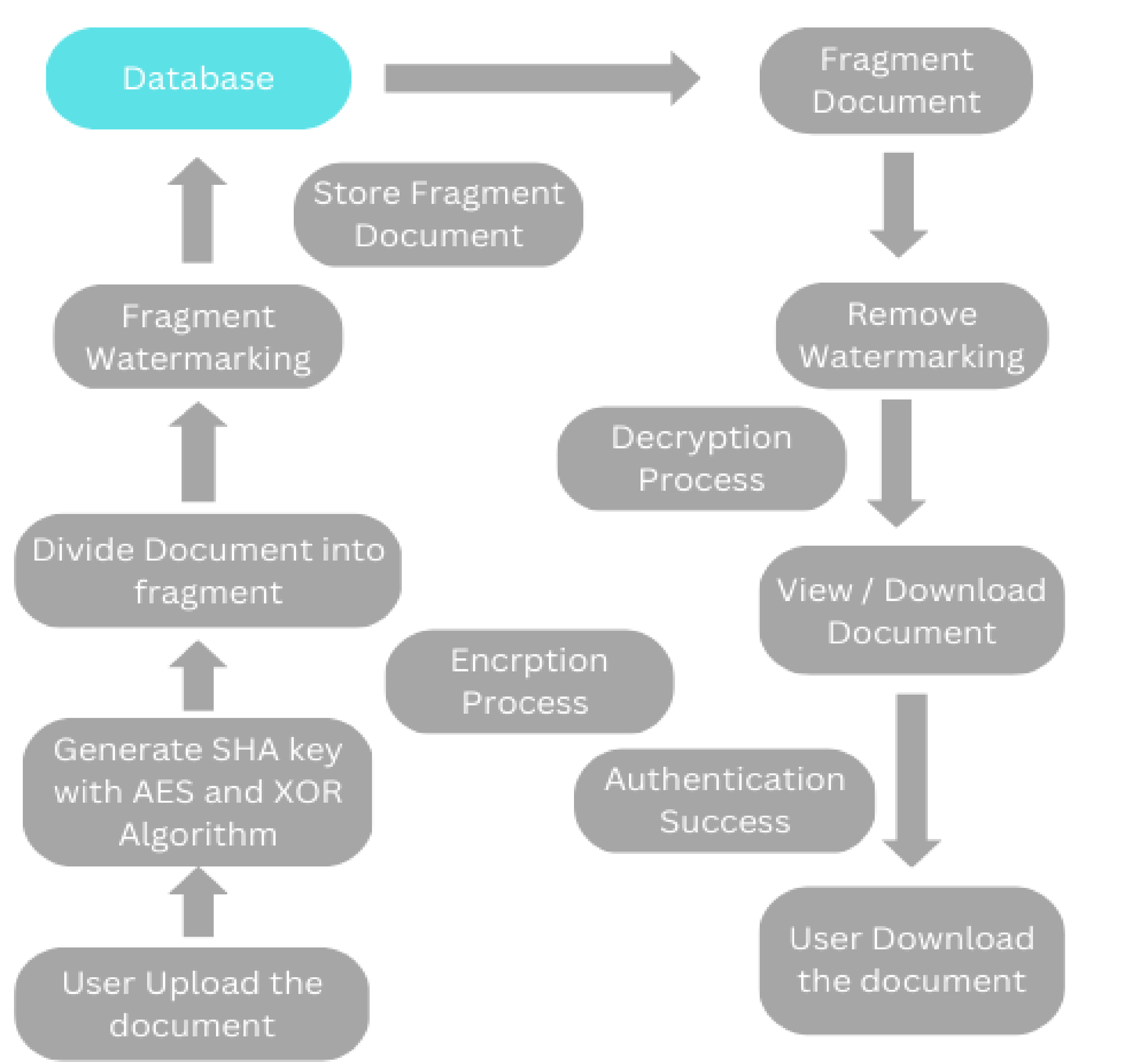
# Architectural Flow Diagram (AFD)



# Data Flow Diagram (DFD)



# Control Flow Diagram (CFD)



# Application of Digital Watermarking

- Protection against unauthorized access
- Copyright Protection
- Authentication
- Brand Protection
- Metadata Embedding

# Demonstrate of this project (Optional)

# Conclusion

In this topic we conclude that digital watermarking is important factor for data security which can protect our data from unauthorized access. It is enhance the data security in the form of digital code which is embedded in user file and verify by digital signature. It is difficult to tamper and misuse of information

# References

[1] A. Anees, I. Hussain, A. Algarni, and M. Aslam “*A robust watermarking scheme for online multimedia copyright protection using new chaotic map*.”Hindawi, Security and Communication Networks, Article ID 1840207 2018 pp 1- 20. Aug. 2017

[2] W. Luo, F. Huang, and J. Huang “*Edge adaptive image steganography based on LSB matching revisited.*” IEEE Trans. On Information Forensics and Security, 5 (2) pp 201-214. Jun. 2010

[3] K. S. Kim, M. J. Lee, H. Y. Lee, and H. K. Lee “*Reversible data hiding exploiting spatial correlation between sub-sampled images*.”Pattern Recognition, 42 (11) pp 3083-3096 Jan 2009

[4] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon “*Secure spread spectrum watermarking for multimedia*..”IEEE Transactions on Image Processing, 6 (12) pp 1673- 1687. Feb 1997

[5] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni “*Reversible data hiding based on wavelet spread spectrum.*”IEEE 6th workshop on Multimedia Signal Processing pp 211-214. Jul. 2004

[6] C. C. Chang, P. Y. Lin “*Adaptive watermarking mechanism for rightful ownership protection.”J. Syst. Software*, 81 (7) pp 1118-1129. May 2008

[7] G. J. Lee, E. J. Yoon, K. Y. Yoo “*A new LSB based digital watermarking scheme with random mapping function.*” International Symposium on Ubiquitous Multimedia Computing pp 130-134. Jun. 2008

[8] W. Luo, F. Huang, and J. Huang “*Edge adaptive image steganography based on LSB matching revisited.*” IEEE Trans. On Information Forensics and Security, 5 (2) pp 201- 214 Mar. 2010

विदर्भ यूथ वेलफेअर सोसायटी, अमरावती

# Thank You………