VERIFYING IMAGE AUTHENTICITY AND RECOVERY USING MERKLE TREE BASED MECHANISM

A Major Project Synopsis
Submitted in Partial Fulfilment of the Requirements for the Degree of

BACHELOR OF TECHNOLOGY
in
Information Technology
(2023-2024)
by

AKASH KUMAR (2007340130007)
KRISHNA PRATAP SINGH (2007340130031)
PRASHANT SHARMA (2007340130042)
SUNDARAM SHARMA (200734130060)

Under the supervision of
Dr GYAN SINGH
(Assistant Professor)
To the
Faculty of Information Technology

Dr A. P. J. ABDUL KALAM TECHNICAL UNIVERSITY
(Formerly Uttar Pradesh Technical University) LUCKNOW
DECEMBER 2023

TABLE OF CONTENT

CHAPTER 1

INTRODUCTION

1.1 Background

Image authentication refers to the process of verifying the integrity and authenticity of a digital image to insure, that it has not been altered, tampered with, or manipulated in any unauthorized way. In recent years the integrity of digital image was protected by several methods like cryptographic image authentication, fragile and semi fragile watermarking. In cryptographic image authentication, there are two operations used one is encryption and second is decryption. Traditional cryptography algorithms exhibit satisfactory results for image authentication with high tamper detection. Drawback of this technique is that hash function is very sensitive means the image is said to be manipulated even when one bit of this image is changed. In watermarking image authentication message or any code has been hidden in the image. The purpose of a watermarking method can vary, but commonly it is used to verify the authenticity or ownership of the image. In our project we are trying to resolve the problem using Merkle Tree based Mechanism and IPFS (Inter-Planetary File System).

AES (Advanced Encryption Standard) is a widely used symmetric encryption algorithm designed to secure sensitive data. It operates on fixed-size blocks of data (128 bits) and supports key lengths of 128, 192, or 256 bits. AES employs multiple rounds of substitution, permutation, and mixing operations to transform plaintext into ciphertext, providing a high level of security for data communication and storage. We can take help of AES encryption algorithm to encrypt the block of pixels we generate.

The project suggests using technologies like the Inter-Planetary File System (IPFS) and blockchain, which is famous for cryptocurrencies like Bitcoin, along with Merkle trees. This combination aims to create a secure and decentralized system for managing and verifying digital image integrity. The proposed method doesn't rely on a single trusted party; instead, each node in the blockchain network can independently verify the integrity of images, making it a more reliable and tamper-resistant approach.

Validation of fake or real images is very important in various scenarios like:

- **Digital forensic:** In criminal investigation images are used as evidence.
- **Authentication in Online Platform:** Image authentication can be useful in online platforms where users upload images, such as social media or e-commerce websites. This helps prevent the spread of fake or manipulated images.
- **Art and Cultural Heritage Preservation:** In the art world, where the authenticity of paintings and artifacts is crucial, image authentication can be used to verify the integrity of digital representations of these items.

And more types of examples in real world scenarios which have uses of image authentication.

1.2 Problem Statement

Verifying Image Authenticity and Recovery Using Merkle Tree based Mechanism.

1.3 Objective

Our project objectives are given below.

- Generate a new image authentication method based on Merkle Tree.
- User friendly UI so that user can easily upload their image.
- Detect the damaged part of the image if altered.
- Recovery of the damaged part.

CHAPTER 2

LITERATURE REVIEW

Authors and Year	Title	Method	Result Analysis
Adil Hauzia, Rita Noumeir (2007)	Methods of Image Authentication: a survey.	Fragile Watermarking, Semi Fragile Watermarking	Watermarking technique is very easily implemented. But visible watermarks may degrade image quality.
Marakumbi Prakash,) Jayashree V. Khanapuri(2018)	A Study on Image Authentication Methods.	Cryptographic authentication, Robust Image hashing authentication, Watermarking authentication	Watermarking technique constructed based on chaotic maps is more efficient compared to other methods.
Dr Bhowmik, T. Feng, A. Natu, T. Ishikawa, C. Abhayaratne(2018)	The Jpeg-Blockchain Framework For Glam Services.	Blockchain architecture	Verified info is stored in JPEG header and Image stored in multimedia server.
Aravindh Raman, Gareth Tyson(2022)	Design and Evaluation of IPFS.	Peer to Peer distributed network	It stored data on the basis of CID.
B. Padmavathi, S. Ranjitha Kumari(2013)	A survey on performance analysis of DES,AES and RSA.	Encryption and Decryption Techniques	AES is mostly used and also more secured than others.
Prof. Dr. Johanners Buchmann Supervised by Erik Dahmen (2007)	Merkle tree traversal techniques.	Merkle Tree	Classical traversal of Merkle tree.

CHAPTER 3

PROPOSED WORK

Proposed methods are divided into several steps:

3.1 Image breaking

We divided the image into N number of block of pixel using image processing library that based on Grid based algorithm.

3.2 Encryption on the image

We use AES encryption algorithm to encrypt of block of pixels generated by above 3.1 process described.

3.3 Upload on IPFS

After encryption of block of pixel, we have finally upload into IPFS (Inter-Planetary file system) as distributed data storage. IPFS is open source, peer to peer distributed hypermedia protocol use for storing and sharing data in a distributed file system.

3.4 Generation of Merkle Tree

We use IPFS content as a transaction and generate Merkle Tree from these transactions. Merkle tree is a tree in which every leaf(node) is labelled with the cryptography hash of a data block, and every node that is not leaf (inner node) is labelled with the cryptographic hash of the labels of its child nodes.

3.5 Image Verification

In the image verification step we just take help of root of Merkle tree. If root of changed or damaged and original image are same then we can say that image is not damaged hence verification step is done.

3.6 Image damaged part detection

This part is done by comparison of Merkle tree of original image with Merkle tree of altered or damaged image recursively.

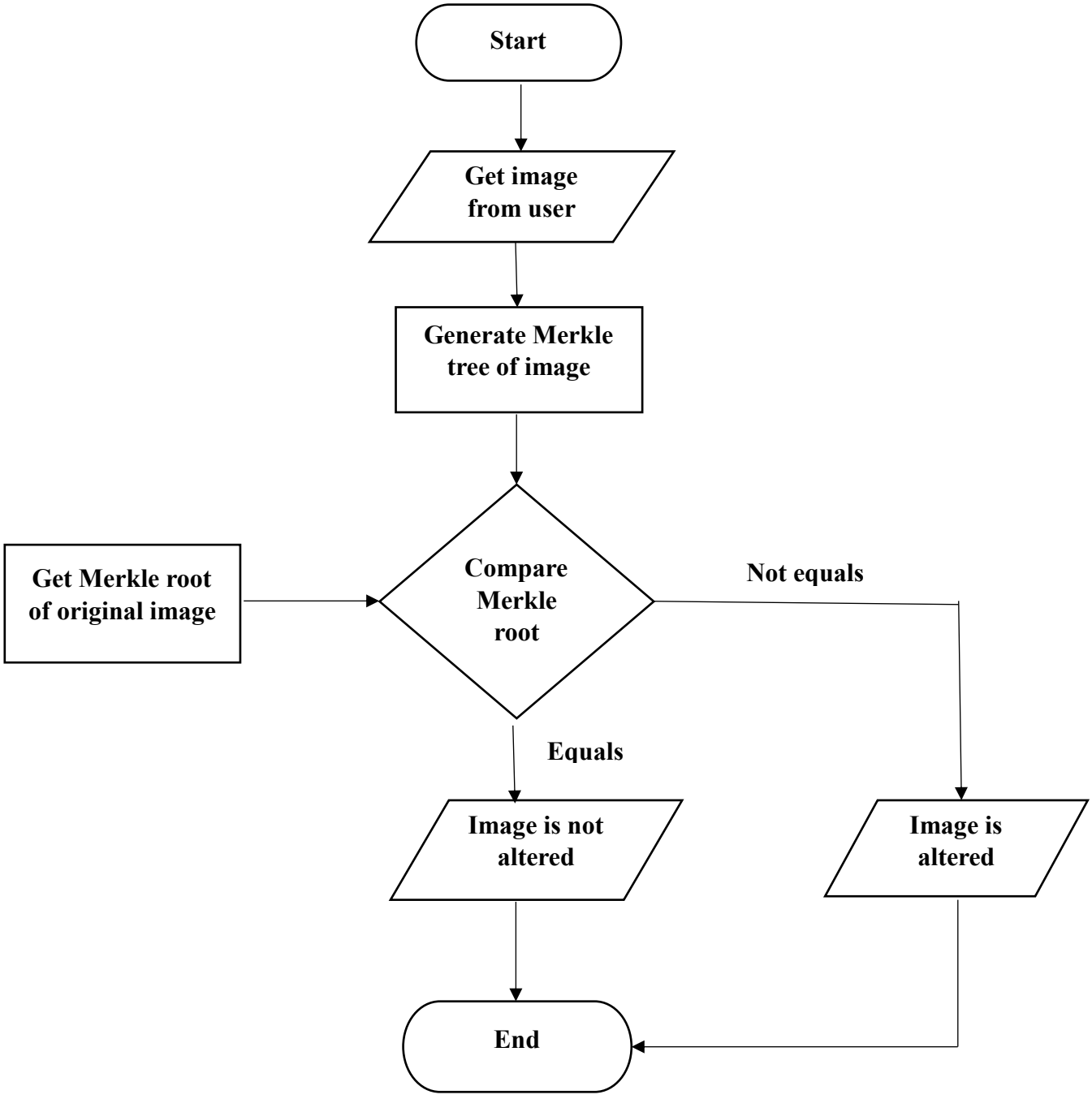
3.7 Image Recovery

We fetch the damaged part of image from previously stored in IPFS.

CHAPTER 4

WORK FLOW CHART

4.1 Flow Chart of Verification of Image



CHAPTER 5
TECHNOLOGY REQUIRED

5.1 Technology

Frontend: React Js

Backend: Express Js

Database: MongoDB, IPFS (Inter-Planetary file system)

Image Processing Library: Open CV

Data Structure: Merkle Tree

CHAPTER 6

CONCLUSION

6.1 Conclusion

By the above describe proposed method our software can able to securely store the image of user so that if any changes or damaged occurs on the image then our software are able to detect the damaged part of the image and also perform the recovery of that damaged part. That's make user to guarantee that their images are kept secure and no one can change