

Detection Of Tampering In Multimedia Using Blockchain

A Project Report

submitted in partial fulfillment of the requirements for the award of Degree
of

**Bachelor of Technology in
Mathematics and Computing**

Under the supervision of

Mr. Jamkhongam Touthang

(Assistant Professor , Mathematics and Computing Department)

Submitted By:

ABHISHEK SINGH(2K17/MC/007)

ADARSH KUMAR (2K17/MC/009)



Department of Mathematics and Computing

Delhi Technological University

(Formerly Delhi College of Engineering)

DECLARATION

We **Abhishek Singh** 2K17/MC/007 and **Adarsh Kumar** 2K17/MC/009 hereby certify that the work which is presented in the Project entitled “**Detection of Tampering in Multimedia Using Blockchain Technology**” in requirement for awarding B.Tech Degree and submitted to the Discipline of Mathematics & Computing, Delhi Technological University (Formerly Delhi College Of Engineering), is legitimate work during period from January 2021 - May 2021, under the guidance of **Mr. Jamkhongam Touthang (Assistant Professor, Mathematics & Computing Department)** .

We certify that whatever we have submitted in this report has not been submitted before for any other purpose

SIGNATURE

ABHISHEK SINGH	2K17/MC/007
ADARSH KUMAR	2K17/MC/009

ACKNOWLEDGEMENT

“The successful completion of any task would be incomplete without accomplishing the people who made it all possible and whose constant guidance and encouragement secured us the success.”

Firstly, we are thankful to God who gives us strength at each step. We are thankful to **Mr. Jamkhongam Touthang** (Assistant Professor, Mathematics & Computing Department), Delhi Technological University (Formerly Delhi College of Engineering), New Delhi and all other faculty members of our department, for their guidance, constant encouragement and sincere support for this project work.

We want to sincerely thanks, **Mr. Jamkhongam Touthang** (Assistant Professor, Mathematics & Computing Department) for giving us the opportunity to work on this Project.

SUPERVISOR CERTIFICATE

This is to certify that **Abhishek Singh (2K17/MC/007)**, **Adarsh Kumar (2K17/MC/009)** , the bona fide students of Bachelor of Technology in Mathematics And Computing Engineering of Delhi Technological University (Formerly Delhi College Of Engineering), New Delhi of 2017–2021 batch have completed their project entitled “**Detection of Tampering in Multimedia Using Blockchain**” under my supervision. It is further certified that the work done in this dissertation is a result of candidate’s own efforts. I wish them all success in their lives.



Mr. Jamkhongam Thouthang

Supervisor

ABSTRACT

A blockchain technology based decentralized multimedia sharing system is proposed to detect and prevent tampering in multimedia. In this digital age, we are increasingly dependent on multimedia material, particularly digital images and videos, to provide accurate evidence for occurrence of events. However, the existence of many advanced yet user friendly content editing tools has led to rethink about the credibility of such content. Our current net is an online source of knowledge. It is based on the concept of repeating and distributing info. Be it video, email, or article. All of those are copies of the original. For instance, if you wish to look at a video on YouTube or receive an online educational certificate of accomplishment, you are actually accessing a digital copy of the initial, not the original one. This is how you see your daily feed on Instagram and twitter, even for media on WhatsApp the concept is the same throughout the internet. One is susceptible to receiving false information. The whole multimedia system is so vulnerable to unwanted media modification. So, the important question here is: Where does the problem lie? The problem is basically the whole structure on which the current internet is based. The structure we use to share media is not good enough. The problem of tampering in multimedia could be seen in all walks of life. Be it in business, politics, economy, education or entertainment. In this article we propose a “difference hash algorithm” based multimedia blockchain framework that will address this kind of issue. First we will be calculating the difference hash value of the two pictures separately. Then we will calculate the hamming distance of two pictures' difference hash value and judge the similarity of two pictures by the size of the hamming distance.

TABLE OF CONTENT

<i>Declaration</i>	<i>ii</i>
<i>Acknowledgement</i>	<i>iii</i>
<i>Certificate</i>	<i>iv</i>
<i>Abstract</i>	<i>v</i>
<i>Table of Contents</i>	<i>vi</i>
<i>List of Figures</i>	<i>vii</i>
Chapter1: Introduction	1
Video Fraudulence	4
Blockchain.....	6
Motivation.....	11
Contribution.....	12
Chapter 2: Methodology	13
Blockchain	13
Advanced Encryption Algorithm.....	14
Message Digest 5.....	15
Proposed Approach.....	16
Chapter 3: Implementation Results	20
Chapter 4: Conclusion	31
References	32

LIST OF FIGURES

Figure 2.1: Centralized vs. Peer to Peer Downloading

Figure 2.2: calculate the dHash value

Figure 2.3: After Scaling to 9*8 resolution

Figure 2.4: After Graying

Figure 3.1: Front View of the Model

Figure 3.2: Node Creation

Figure 3.3: Message Displayed

Figure 3.4: User Login

Figure 3.5: Message Displayed

Figure 3.6: Upload Video

Figure 3.7: Original Video Snapshot

Figure 3.8: Uploading Video

Figure 3.9: Message Displayed

Figure 3.10: Upload Video

Figure 3.11: Status of the video

Figure 3.12: Node creation

Figure 3.13: Message displayed

Figure 3.14: User Login

Figure 3.15: Message Displayed

Figure 3.16: Fraud/Tempered video Snapshot

Figure 3.17: Upload Video

Figure 3.18: Message Displayed

Figure 3.19: Video Status

CHAPTER 1

INTRODUCTION

Blockchain is associated encrypted, distributed info that records knowledge, or in different words Benefits of Blockchain Technology is magnified time effectiveness because of the period of time transactions, Direct Transactions eliminate the overheads and treater prices, Reduced risks associated with cybercrimes, frauds and change of state, additional clear processes with a correct record creation and trailing, extremely secure because of scientific discipline and decentralized Blockchain protocols Blockchain technology may be employed in numerous industries like digital currency, Healthcare, Government. within the monetary services sector.

Blockchain technology will play a key role within the and ability of the tending knowledge. It holds the potential to handle several ability challenges within the sector and modify secure sharing of tending knowledge among the varied entities and other people concerned within the method. It eliminates the interference of a third party and conjointly avoids the overhead prices. With Blockchains, the tending records may be hold on in distributed knowledge bases by encrypting it and implementing digital signatures to confirm privacy and credibleness.

Blockchain technology holds the ability to remodel Government's operations and services. It will play a key role in up the information transactional challenges within the Government sector, that works in siloes presently. the right linking and sharing of knowledge with Blockchain modify higher management of knowledge in the retail sector This includes from guaranteeing the credibleness of high worth product, preventing, deceitful transactions, locating purloined things, sanctionative virtual warranties, managing loyalty points and streamlining offer chain operations.

This paper proposes a structure by utilizing compelling hashing procedures to guarantee the security of the information.

In Internet of Things (IoT) environments Blockchain has indicated an incredible potential for setting up trust and accord components without contribution of any outsider. Understanding the relationship among correspondence and blockchain just as the presentation requirements presenting on the partners can encourage structuring a devoted blockchain enabled IoT frameworks. we can set up a diagnostic model for the blockchain-empowered remote IoT framework. By considering spatio-transient area Poisson appropriation, i.e., hub topographical dissemination in spatial space and exchange appearance rate in time space are both demonstrated as Poisson point process (PPP), we first infer the conveyance of signal-to-impedance in addition to commotion proportion (SINR), blockchain exchange fruitful rate just as generally throughput. In view of the framework model and execution investigation, we structure a calculation to decide the ideal full capacity hub sending for blockchain framework under the measure of augmenting exchange throughput. At last, the security execution is investigated in the proposed systems with three common assaults. Arrangements, for example, physical layer security are introduced and examined to keep the framework secure under these assaults. Numerical outcomes approve the exactness of our hypothetical investigation and ideal hub arrangement calculation.

In this manner, numerous exertion and cost should be contributed to refresh these gadgets once any powerlessness is recognized. In the current brought together IoT framework, a cloud server is essential for the identification, approval, and correspondence among low-end gadgets, bringing about colossal consumption on development and upkeep of servers. blockchain strategy empowers the advancement and financially savvy, exceptionally safe exchange, which is actually the missing piece of the current IoT biological systems. Specifically, blockchain permits the made sure about and dependable transactions, communications between two savvy gadgets without the need of incorporated position, which improves the settlement time from days to practically prompt separated from sparing operator expenses.

Video Fraudulence

Video fraud has become a perilous technique for people for their advantages. The doctored videos are embedded in various platforms for malicious intent. Once they have come on the internet they spread like wildfire, we can see the power of this technique for achieving some malicious purposes.

Technology is constantly evolving and fraudsters are finding new ways to exploit people through this technologies. As we have discussed video fraud is a new and easy technique for achieving their aim. People watch videos regulators either on internet or television. They are brainwashed regularly. So this makes them more vulnerable to fraudsters who are ready to exploit them any second they find.

Fraud affects our life in vary ways. We all have in some time have been accustomed to fraud whether it is a bank fraud or some investment fraud. But when we encounter a fraud we become more aware and more sceptical . Video fraud is a kind of fraud which we even can't find for example we see a video that is doctored , based on that video we made some stand on our mind and we don't even know that video is a fraud. So that's how it works.

Like one of the dangerous frauds is identity theft here the whole identity is the person is used for some malicious intent. Video fraud is kind a similar here fraudster tempers a video so that we think the person whatever is saying is truth and his identity get defamed.

Video fraudulence is an easy way to defame or to plant an idea on someone. So that's why we

have come with this idea of detecting video fraudulence so that the vulnerability become low. It's difficult to detect this kind of fraud because the data is huge and discrepancy is very less. So we have to detect that discrepancy and have to inform the user that this video has some kind of fraud.

There are various techniques which can be used to detect fraud but we had to choose the most reliable which we found was blockchain. It's a new technology which can be very useful for this purpose. We can say blockchain is a advanced form of internet. Here we don't need a central authority we only need various users connected via chain who can exchange information to one another. Here the users also called as nodes compete each other to check the validate of an information which is uploaded by one of the nodes. First one to check get rewarded that's how this chain works.

Blockchain

what is a blockchain. If you think generally, a blockchain is a linked list. So what is a linked list? All of you know that a linked list is a set of blocks which are connected to each other by some kind of a link. In case of a data structure linked list, you have the nodes and nodes are connected by pointers and pointers are basically memory addresses. But, in case of a blockchain the which is replicated at various nodes or various computers and therefore, the linking is not based on memory addresses. So we have a different notion of linking between nodes and each of these nodes are called blocks. So therefore, you can imagine a blockchain as a series of blocks and each block is connected to its previous block by some kind of a link.

it is replicated all over because replication gives you number of different advantages like if one of the replica gets corrupted, the other replicas are there to make sure that the integrity of the information contained in the in the data structure is maintained. And also replication gives you some kind of guarantee of integrity of data.

It is distributed in the sense that the different computers involved in the blockchain platform actually are running distributed algorithms in order to maintain the data's consistency and integrity. And the consistency of the data is maintained by a process called consensus. Consensus means that everybody agrees that the data that goes into the data structure is what they agree to put there.

The linking as I said before, traditional link list the linking is through memory addresses. But in this case, we cannot use memory addresses for linking. So there is a cryptographic technique called hashing. So we actually use something called a hash linking and the integrity of the data is maintained because of cryptography techniques and consensus and replication.

Therefore, blockchain is a data structure that is maintained distributedly and that is replicated and main purpose of blockchain is to maintain the integrity of the data. what is the integrity? Integrity means that the data once it has been agreed by all the relevant parties to put in the data structure, it has not been tampered with it. Nobody has come and changed the data and claim that this is the data that was put in. That is made virtually impossible in a blockchain and that is the main property of the blockchain that it maintains the integrity of the data and as we will see that most of the applications where blockchain is used be it cryptocurrency or be it some other application, the integrity of the data is the main thing in blockchain. So what is blockchain used for? So first of all, you know many times we keep logs of events, right. So when somebody accesses your computer, the computer keeps a log of the user names and how they authenticated themselves. Microsoft Windows gives event logs every event that happens like you open a new program on your machine or something crashes or any kind of event or you know it, you get connected to the internet.

All these events are kept in event logs. So logs are very important. When you do banking transaction bank keeps logs of when you interacted with its banking servers and what you did, what transactions you made, all this are logged.

The main problem with keeping logs without any notion of protection of the integrity is that somebody can tamper with the logs and somebody can delete some of the accesses. And therefore, later on when you check the log, you would know some part of its history.

So therefore, the blockchain is designed in such a way, so that it is an immutable ledger of events, which means it is a log that cannot be changed by a malicious party or by mistake. And therefore, all the data that you put in there could be event logs, it could be transactions, it could be various kinds of accesses and modifications you do to some other thing like a data or you do a property transaction. All these things logs has to be kept in an immutable ledger. And that is what blockchain provides. So and the tampering of this data is made virtually impossible.

The main problem with keeping logs without any notion of protection of the integrity is that somebody can tamper with the logs and somebody can delete some of the accesses. And therefore, later on when you check the log, you would know some part of its history.

So therefore, the blockchain is designed in such a way, so that it is an immutable ledger of events, which means it is a log that cannot be changed by a malicious party or by mistake. And therefore, all the data that you put in there could be event logs, it could be transactions, it could be various kinds of accesses and modifications you do to some other thing like a data or you do a property transaction. All these things logs has to be kept in an immutable ledger. And that is what blockchain provides. So and the tampering of this data is made virtually impossible.

So we do not say it is impossible to tamper, as we will see, as we learn more that there if you have a very high computational power, which is almost impossible for individuals together. But if you can gather that kind of computation power you can actually subvert and this all the protection and change but since it is virtually impossible, we would say that this is a tamper resistant log. And therefore, having these properties, we basically use blockchain as a platform to create and transact cryptocurrency. So cryptocurrency as we will see bitcoin ethereum, these are cryptocurrencies.

And we will see that one of the first application of blockchain was bitcoin. So the whole idea of creating currency, that whose transactions whose creation whose use everything has to be put in a tamper proof log, and without a trusted third party or without a central agency, which keeps track of this logs and it will be clearer as we go into the course. And also you know many people confuse or conflate the idea of bitcoin and blockchain.

And as we will see, that cryptocurrency is just a part of the story. And there are any number of other applications in which we need to keep tamper proof or tamper resistant logs and their blockchain is a very good you know platform.

Ethereum is another such cryptocurrency. Now you will also hear a lot of news like for example, you will hear that United Emirates is fully going on with blockchain for their most of the E-governance applications. Governance means that you know all kinds of things like property registration, and you know car licensing, or you know license, driver licensing all kinds of things they are doing on blockchain. And many other countries are doing the same thing. Same thing

you will hear a lot about supply chain management on blockchain or you will hear energy management especially in case of micro grids, and renewable energy, you will hear a lot about the applications of blockchain or you know electric vehicle charging stations and paying for the, you know electric charging and all that on a blockchain like in Germany. So very soon you will hear that the blockchain is for everything, for Nirvana. So people often say that okay, so this is a new hype and a lot of hyperbole. So what we will see in this course, is that it is not a hype, and it is a technology, quite transformative technology. So many people compare it with the advent of the Internet in transforming our lives and digitalization. And similarly, people say that or predict that blockchain is going to be as transformative in the way we digitalize our functioning and our governance and our industrial dealings or financial markets and so on so forth. So even if you do not care about cryptocurrency and its market volatility, which is one of the biggest criticism of cryptocurrency, you will see a lot of application of blockchain which has nothing to do with cryptocurrency.

will try to teach you why that is the case. And in fact, I personally is a strong critic of cryptocurrencies like bitcoin and others. And therefore, my interest is that people learn that even if you do not care about cryptocurrency, you should care about blockchain as a technology, because it is a transformative technology.

the other thing is that most of this bitcoin mining companies, now actually there are companies which actually can only afford such large-scale bitcoin mining and this many of these companies are in China. Now what happens is that it is provable, that if one person or one player in the bitcoin platform has more than 51% of the computational power, then he can actually completely change the data in the bitcoin network.

So earlier we said that in a blockchain, the data that we store after a consensus is tamper proof, right. Nobody can come and change the data. The reason why they cannot do that because to the amount of computation they have to do, in order to tamper it is too much because they have to then undo all the computation that was done to store that data and any other computation that was done to store data subsequent to that.

So this is an total amount of work, computational work that somebody has to do to tamper with. But if I have majority of the computing power in the entire ecosystem, then I can actually

completely change the entire chain, chain of data, all the data I want to change and all subsequent data. Now think about this.

If one country has most of these or majority of these companies who are doing bitcoin mining, if they want to get together and then their total computational power becomes above 51%, then bitcoin will have no integrity of its transactions. And therefore the entire ecosystem will fail.

Also because of these environmental concerns and volatility of the cryptocurrency and so on, we may be the country in which all these companies are there and they are consuming power, they are polluting the environment, the country might decide that they will curtail the activities of these companies and therefore, there will be another kind of problem. And when this kind of news has come, you will see the bitcoin prices fall.

The reason is, even though it may be a speculative news, because we are now dependent on all these different extraneous things which are not imagined by the originator of the bitcoin and the originator of the bitcoin was an anonymous person who used the name, Satoshi Nakamoto. And in 2009, he wrote the first you know version of the bitcoin and he launched it and he also wrote a white paper. And his idea was to get rid of the tyranny of the large banks, right. So in 2008, there was an international financial meltdown and it turned out that the banks did a lot of things which are not properly you know correct things to do. And in fact, from the writing and from the original message that was in the first block of the bitcoin blockchain, it seems like he was actually trying to emancipate people from the, from the hold of the banks.

And then they want the entire world everybody to become part of a currency system, which is not dependent on a central bank or on the banks to actually decide the, you know the value of the money. But unfortunately, the way it worked out and the way it unfolded is that only a handful of companies are now doing most of the bitcoin mining.

And then all the transactions that are happening are also by only a you know only 1, 2% of the people who are involved in the bitcoin ecosystem. And the same thing is happening in ethereum that 90% of the transactions are done by maybe hundred players when there are about 6 million players in the ecosystem. So you can see that there is a huge amount of inequality that is

building up in the cryptocurrency system when there are only handful of players who are doing all the activities, all the transactions storing all the currencies, and the rest of the other people are doing very little. And therefore, the entire dream of Satoshi Nakamoto whoever he is, is not being translated to reality. So that is another problem.

And as we know that in India, the RBI has put a blanket ban on bitcoin as a transaction medium and or any kind of cryptocurrency and there is a good reason for that, and we will not get into that, but that is how it is. So then there is another problem. That this problem has been happening because of various reasons.

Blockchain was invented by an individual or a group of persons by pseudonym Satoshi Nakamoto, who first used the concept of the blockchain for a cryptocurrency Bitcoin. The invention of Blockchain made this as the first technology that solves the double spending problem without needing a third party or a central authority. With the invention of Blockchain, its applications are increasing at very high speed. It's popularity is increasing as of the Internet in the 1990's. It's applications are manifold and it is used in many areas such as healthcare, cryptocurrency, industries etc.

Motivation

For instance in Gujarat, there was a fake video in which a political party leader was threatening people from outside the Gujarat that they are illegal residents and are committing rapes and murders. This lead to violence where people of Gujarat were beating people from outside Gujarat, mostly from Bihar and Uttar Pradesh, doing small works like laborers and on farms.

Contributions

We have used some cryptographic protocols as cryptography is the technique for secure communication between two parties without any interruption from any third party. Cryptography uses several protocols to encrypt the message from the sender's side, this is used

to authenticate that no one is reading the message in between. From here we took the idea that we can also encrypt our video in a way that it uses the property of binary digits and it will generate a unique id for the video. We have used MD5 cryptographic algorithm for the encryption of video on binary digits. Moreover, we will use Blockchain technology for video fraud detection so that multiple systems across the network may detect if a video stored on any node is forged.

CHAPTER 2

METHODOLOGY

In this section we briefly describe the method we have used to achieve the results, that is ‘a contextual framework’ based on our research, a method to detect tampering in media. The whole process is purely based on how similar the given two images are. For finding the similarity we will perform two steps which are briefly described below, first ‘difference hash value’ of two images are calculated, then using the difference hash value, hamming distance will be calculated. Using that we will decide how similar the given images are.

Blockchain

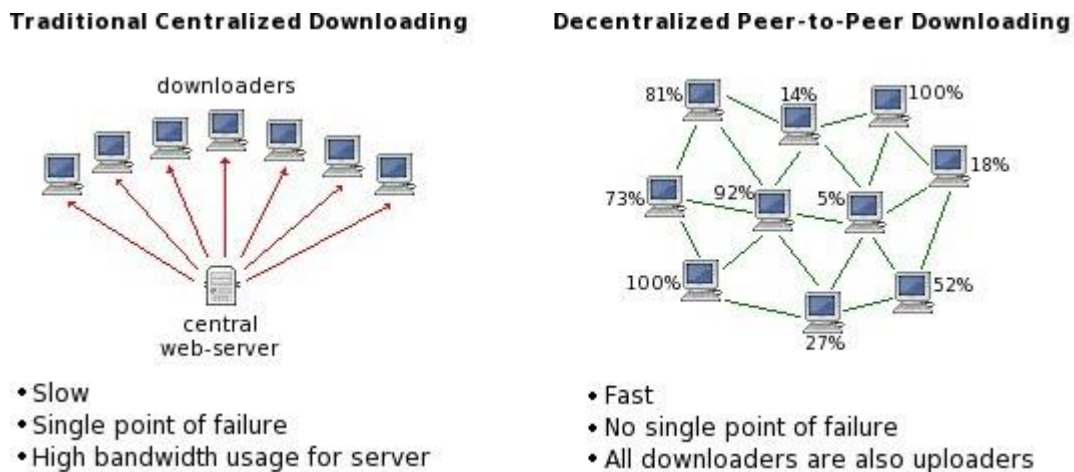


Figure 2.1 Centralized vs. Peer to Peer Downloading

As we can see from the above figure, Traditional Centralized systems lacks many things. They are slow and the biggest accountability is of the single point failure. If the Central system is compromised or destroyed then everything is finished, whereas in decentralized system, if one system is failed or compromised, it doesn't mean that entire system is at risk. Only that particular node is destroyed, everything else is running smoothly. With blockchain (peer to peer network), the information is distributed across the nodes. The control of

information is decided by the consensus of the majority of the nodes in the network. The data that was first at a central point, now is shared by many users who are present on the blockchain. Data Transparency is also a factor which is provided by the blockchain. The data that is to be shared should be tamper proof. With Blockchain the data is not at a central point but it is shared by the trusted entities and the forgery done by any node can be easily detected.

Security is also a main factor and Blockchain works in a very efficient way to provide security.. Cryptographic functions are strong one way functions that generate digital checksum on digital data so that it can't be extracted. This makes Blockchain a secure decentralized platform for various applications.

There are also some challenges faced by the blockchain such as scalability and confidentiality. In blockchain all data is visible to all the nodes so contain very big data such as big video files in GB's so the storing of this amount of voluminous data is complex. Another challenge is that the Blockchain technology is quite new. It is understandable by very few persons and to implement this they have to change their way of working entirely which can be difficult for some persons. Another problem is there is no defined standard for it. This technology is continuously evolving making it harder for the people to adapt to it. Until this technology become quite standard it will be very difficult for individuals and organizations to adapt this technology. But as we are going forwards we can see that this technology can bring a enormous change not just to some software but to the lives of the people where this technology can solve various problems.

In our whole work, we will be creating nodes on a network. The nodes are basically some users in this network. By sending hash to everyone we are creating a system where the fraudulence in the video can be detected, we are achieving this by creating a hash and sending it to every node.

Advanced Encryption Algorithm

Advance Encryption Algorithm is used in our project for password protection in nodes. Advance Encryption Algorithm is defined as a block cipher with block length of 128 bits or 4 word plain text. Number of rounds used in Advance Encryption Algorithm is 10 rounds and each and every round uses separate keys. The key size in every round in Advance Encryption Algorithm is 128 bits or 4 words or 16 Bytes whereas length of one word is 32 bits. The number of sub keys used in Advance Encryption Algorithm is 44 sub keys and each sub key length is 32 bits or one word or 4 Bytes. Advance Encryption Algorithm uses 4 sub keys in each round of length of 128 bits or 4 words. Advance Encryption Algorithm uses 4 sub keys in pre-round calculation of length 128 bit or 4 words. At the last we got Encrypted cipher text of length 128 bits or 4 word 16 bytes. If we observe the single round of the AES in starting, plain text of length 128 bits is applied to add round keys which uses 4 sub keys. After the add round key, next apply substitute bytes, which are also called S-box in AES where input and output is of length of 128 bits. After the substitute bytes, we apply the shift rows, it simply means just applying circular right shift operation and here input and output is of length 128 bits. After shift rows, we apply mix column of same input and output length, then output given to the add round key which also uses 4 sub keys. This is round one. Further 9 rounds are same as this round then we get a cipher text.

Message Digest 5

MD5 compressed any large length input data into a fixed 128 bit length output data. we studied the working of MD5 as first we find the length of the padding before padding we append the original length. We add padding into a original message in such a way that the total length is exact 64 bit less than exact multiple of 512.

We find the padding then we divide the total input length of original message into 512 bit blocks which further divides into 16 32-bit sub blocks. Initialized the chaining variables A1,B1,C1,D1 and initialize all these with hexadecimal values.

Now we process blocks in that manner then there is a loop which execute many blocks of 512 blocks. First of all copy the chaining variables A1,B1,C1,D1 into a corresponding variables a1,b1,c1 and d1. Process into 4 rounds of all the 16 sub blocks.

The output of the MD5 algorithm is a set of four blocks of 32 bit which make total 128 bit fix message digest output.

Proposed Approach

SIMILAR IMAGE DETECTION STEPS:

- Calculate the Difference Hash value of the two images separately.
- Calculate the Hamming Distance of the two images by difference Hash value, and judge the similarity of the two images by the size of the Hamming distance.

Difference Hash calculation



Figure 2.2 The picture that needs to calculate the dHash value

Zoom picture

On the off chance that we need to ascertain the dHash esteem in the figure over, the initial step is proportional to an adequately little size. For what reason do you have to zoom? Since the goal of the first picture is by and large extremely high. A 200*200 picture has an entire 40,000 pixels, and every pixel holds a RGB esteem. 40,000 RGB is an enormous measure of data, and numerous subtleties should be handled. Along these lines, we need to zoom the image to a minuscule size, conceal its subtleties, and just see the woodland yet not the trees. That is we need to zoom the image / picture enough to the pixel level so that each and every pixel and its adjacent pixel will be clearly visible, their size and color. The suggested scaling is 9*8. In spite of the fact that it very well may be scaled to any estimate, this worth is generally sensible. What's more, the width is 9, which is useful for us to change over to the hash esteem, look beneath you will comprehend.

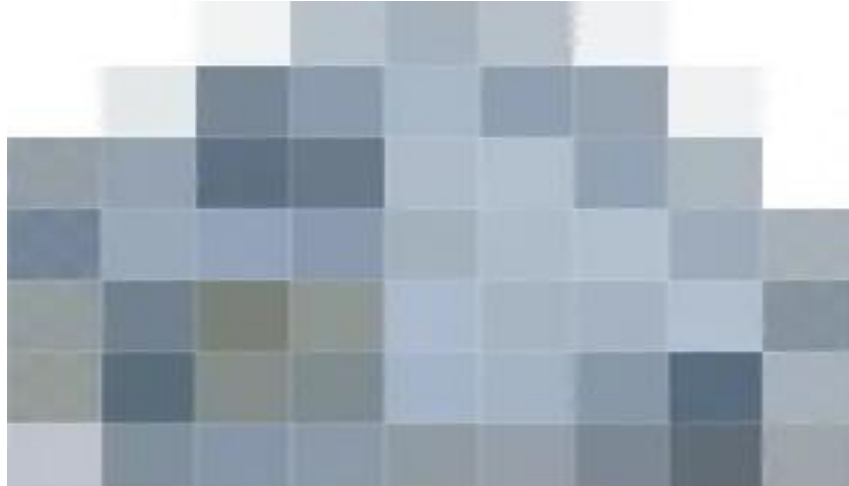


Figure 2.3 After scaling to 9*8 resolution

Graying

The full name of dHash is the distinction esteem hash, which is calculated by getting the shading power contrast between two contiguous pixels. The subtleties of our zoomed picture have been covered up and the measure of data has gotten less. Yet, it isn't sufficient, on the grounds that it is huge and comprises RGB esteems. White is addressed as (255,255,255), and dark is addressed as (0,0,0). The bigger the worth, the more brilliant the tone, and the more modest the hazier. Each tone is made out of 3 qualities, in particular the red, green, and blue qualities. In the event that you straightforwardly utilize the RGB worth to think about the shading force distinction, it is very confounded, so we convert it into a dim value just a number from 0 to 255 addresses the dim. For this situation, the three-dimensional correlation is streamlined to a one dimensional examination.

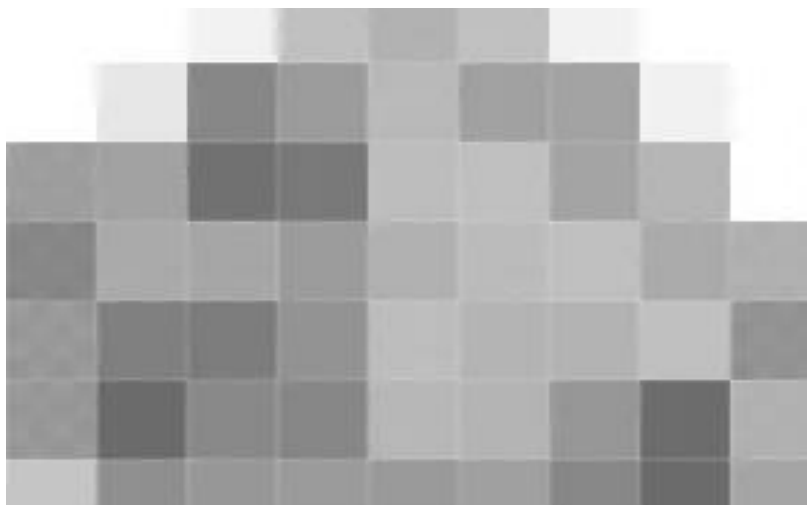


Figure 2.4 After graying

Difference Calculation

The distinction esteem is calculated by computing the force correlation of adjoining pixels present in each line. Our image has a goal of 9×8 , so there are 8 columns, each with 9 pixels. The distinction esteem is completed for each line independently, which is to ensure that the principal pixel in the following line won't be in contrast with any pixel in the primary column. There are 9 pixels in each column, at that point 8 contrast esteems will be created, which is the reason we pick 9 as the width, in light of the fact that 8bit can simply shape a byte, which is advantageous to change over to hexadecimal worth.

On the contrary if the shading force of the past pixel is more recognized than the subsequent pixel, at that instant the distinction esteem is set to True(that is, 1), while in case when it isn't distinguishable than the subsequent pixel, it is put to False(that is 0).

Convert to Hash Value

We treat each worth in the distinction esteem cluster as a piece, and every 8 pieces structure a hexadecimal worth, and link the hexadecimal qualities and convert them into a string to get the last Difference Hash esteem.

Calculate Hamming Distance

The idea of Hamming distance isn't just utilized in the field of picture correlation, yet in addition in numerous fields. For a particular presentation, kindly allude to Wikipedia. The Hamming distance demonstrates the number of steps are expected to adjust A to B. For instance, for the strings "abx" and "ab3", the Hamming distance is 1, since you just need to change "x" to "3". The Hamming distance in 'difference-hash' is the quantity of changed pieces by figuring the distinction esteem. Our distinction of esteem is addressed by 0 and 1, which can be viewed as two fold. The Hamming distance between two fold 0110 and 0111 is 1.

We convert the difference Hash estimation of the two pictures into a two fold contrast and take a XOR. The quantity of digits of "1" in the computation of the XOR result, that is, the quantity of various digits, is the Hamming distance. On the off chance that the info boundary isn't the difference Hash estimation of the two pictures, yet straightforwardly analyzes the two pictures, at that point there is no compelling reason to create the difference Hash esteem, and straightforwardly utilize the distinction exhibit in Step3 to check the various digits, which is the Hamming distance. As a rule, the Hamming distance is under 5, which is essentially a similar picture. You can pass judgment on the basic benefit of Hamming distance dependent on your genuine circumstance.

CHAPTER 3

IMPLEMENTATION RESULTS

In this section, we show the snapshots of the results from the proposed model.



Figure 3.1: Front View of the Model

1. In the first Window, We can see the two options: one is Node and other one is Create Node. If the user is registered on the network then he just have to log in. If he is not registered then first he has to register himself by clicking on Create Node.



The image shows a window titled "New Create Node". Inside the window, there are three input fields: "Name Node" with the text "Abhishek", "Password" with masked characters "*****", and "Node Details" with the text "personal". Below these fields is a button labeled "NEW NODE".

Figure 3.2:Node Creation

2. The user can register himself on the network by providing details such as name of the Node or User , Password and details of the Node. Once he has entered all his details he has registered himself successfully by clicking on the New Node.



Figure 3.3: Message Displayed

3. A message will pop up telling us that the record is successfully inserted.



The screenshot shows a web application window titled "Video Fraud Detection Using Blockchain". It features a login form with two input fields: "User Id" containing the text "Abhsihek" and "Password" containing six asterisks "*****". Below the password field is a "Login" button. The window has a standard title bar with minimize, maximize, and close buttons.

Figure 3.4 : User Login

4. Once someone has registered on the Network, he can Login by writing all the credentials in the given fields and can press on Login Button.



Figure 3.5 : Message Displayed

5. A message will pop up telling us that our credentials are verified and our login has been successful.



Figure 3.6 : Upload Video

6. Now on a node in the Network, we can upload a video. In this window we will click on New Upload Video because yet no video has been uploaded yet. So we can't click on check Video status because there is no video whose status we can check.



Figure 3.7: Original Video Snapshot

7. First we upload the original video in which there is no fraud.

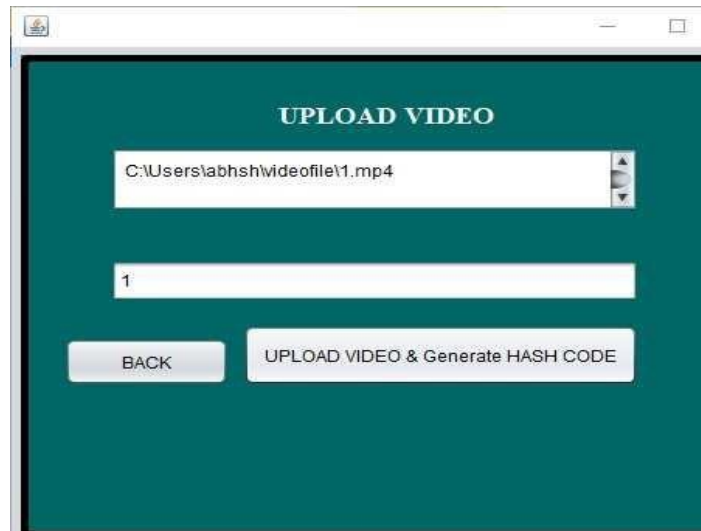


Figure 3.8: Uploading Video

8. We can upload a video by providing a path to the video. Once we have provided the path we can upload it and we will generate hash code of the video. Second tab tells us the id of the video.



Figure 3.9: Message Displayed

9. A message will pop up telling us that our video has uploaded successfully and the hash is generated successfully.




Figure 3.10 : Upload Video

10. Now we go back to the window where we will click on the Check Video Status to see that has our video been uploaded and generating a hash properly.



Figure 3.11: Status of the Video

11. We can see by clicking on the view status that our video status is okay which means it has not been tempered with. We can also see the hash of our video which is a 128 bit hexadecimal number.



New Create Node

Name Node:

Password:

Node Details:

NEW NODE

Figure 3.12 : Node Creation

12. Now a attacker comes on the network so first he has to register himself by providing his details and then he is also a part of the network.



Figure 3.13 : Message Displayed

13. So he has successfully entered on the network.



Figure 3.14 : User Login

14. Now he will login so that he can also upload a video.



Figure 3.15 : Message Displayed

15. So he has login successfully by providing all the credentials.

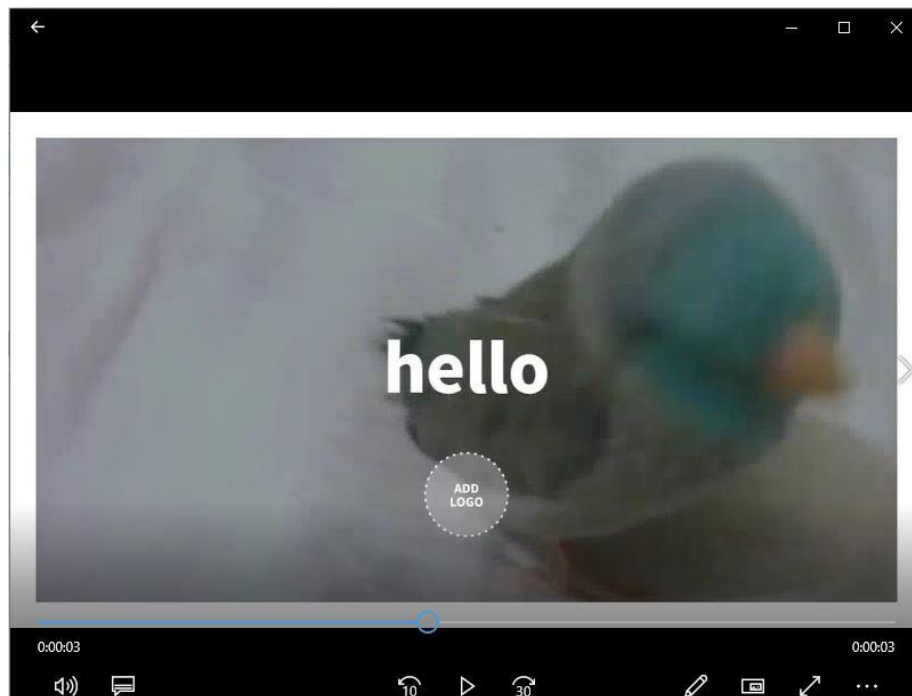


Figure 3.16 : Fraud / Tampered Video Snapshot

16. Now the attacker has uploaded a fraud / tampered video. He has forged the original video. Here we can see that he has added a text.

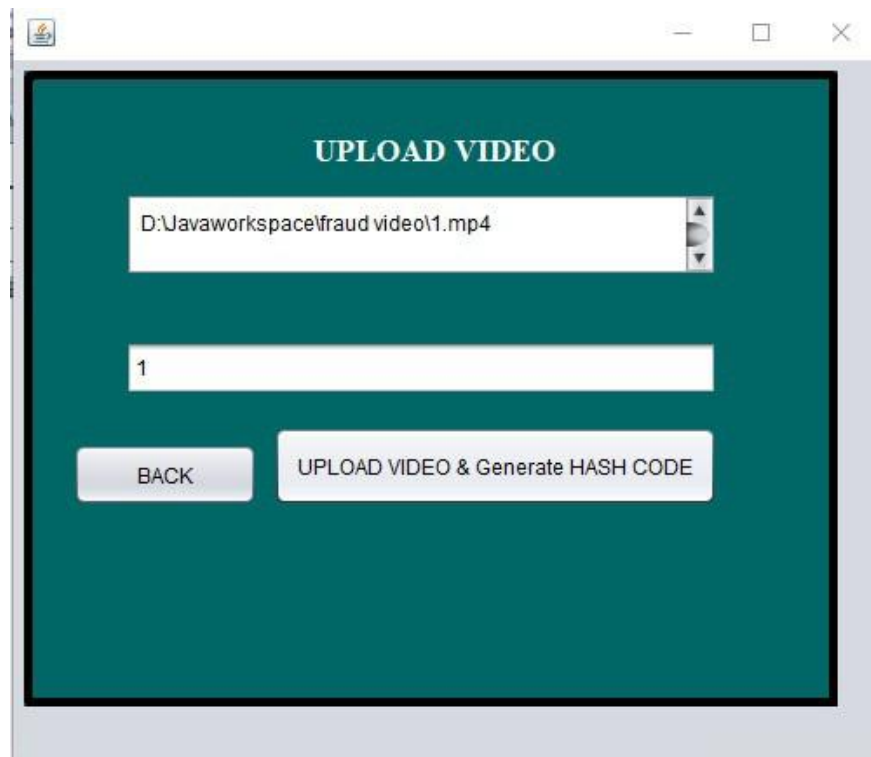


Figure 3.17 : Upload Video

17. Now he is uploading the video. It is the same video that the first user has uploaded but he has forged this video. The video is changed.



Figure 3.18: Message Displayed

18. The video is uploaded successfully and the hash is also generated. Now Anyone on the network can view the status on the universal ledger which is accessible by all.



Figure 3.19: Video Status

So This is how Our GUI is working. We will create the entire blockchain network in our future work and will present a full-fledged chain of blocks detecting video frauds.

CHAPTER 4

CONCLUSION

In this paper we proposed another dispersed and altered conformation media exchange structure dependent on the blockchain model. The proposed Multimedia Blockchain structure is based on a Difference Hash calculation that employs Hash to distinguish any altering and to recover the first substance. We have effectively shown the confirmation of this idea.

We have successfully recognized tampering of images so far. This work of field can be extended for identifying tampering of videos on social media. A video is defined as the collection of many images. Let's say that a video consists of n images. We create an array of size n starting from 0 to $n-1$ storing images. Next, we store the hash created for each of these images stored in another array A . Eventually, we create the hash of the video at a later stage of time after it has been shared to multiple places, which might or might not be tampered. We store these hashes in an array called B . Next we compare the hashes stored in $A[t]$ with $B[t]$, where t ranging from 0 to $n-1$. If any of the hashes don't match, we can easily say that the video is tampered.

At present, we have been using a different hash algorithm. In future, we plan to work on developing other algorithms which will provide better efficiency and accuracy.

REFERENCES

1. The impact of counterfeit drugs in south and south-east Asia, Available: <https://www.europeanpharmaceuticalreview.com/article/92194/the-impact-of-counterfeit-drugs-in-south-and-south-east-asia/>
2. Hasan et al. , “A Blockchain-Based Approach for the Creation of Digital Twins”, IEEE Access, vol. 8, pp. 34113-34126, 2020.
3. C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," IEEE Internet of Things Journal, vol. 7, no. 2, pp. 818- 829, 2020.
4. C. Zhanget al., "BSFP: Blockchain-Enabled Smart Parking With Fairness, Reliability and Privacy Protection," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6578-6591, 2020.
5. X. Liu, S. X. Sun and G. Huang, "Decentralized Services Computing Paradigm for Blockchain-Based Data Governance: Programmability, Interoperability, and Intelligence," IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 343-355, 2020.
6. S. Seven, G. Yao, A. Soran, A. Onen, and S.M. Muyeen “Peer-to-Peer Energy Trading in Virtual Power Plant Based on Blockchain Smart Contracts” IEEE Access, vol. 8, pp. 175713-175726, 2020.
7. V. Jaiman, and V. Urovi, “A Consent Model for Blockchain-Based Health Data Sharing Platforms” , IEEE Access, vol. 8, pp. 143734-143745, 2020.
8. H. Guo, W. Li, M. Nejad and C. C. Shen, “Proof-of-Event Recording System for Autonomous Vehicles:A Blockchain-Based Solution”, IEEE Access, vol. 8, pp. 182776-182786, 2020.
9. X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, “Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities”, Future Generation Computer System, vol. 112, pp. 859-874, 2020.
10. Y. Yuan and F. Wang, "Towards blockchain-based intelligent transportation systems,"in IEEE 19th International Conference on Intelligent Transportation Systems, pp. 2663-2668, Brazil, 2016
11. E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer and C. Weinhardt, “A blockchain-based smart grid: towards sustainable local energy markets”, Computer Science-Research and Development, vol. 33, pp. 207-214, 2018. 32 [12] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, “EduCTX: A Blockchain-Based Higher Education

12. M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "EduCTX: A Blockchain-Based Higher Education ,Credit Platform", IEEE Access, vol. 6, pp. 5112-5127, 2018.
 13. J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira and A. Akutsu, "The Blockchain-Based Digital Content Distribution System," IEEE Fifth International Conference on Big Data and Cloud Computing, pp. 187- 190, China, 2015.
 14. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," IEEE 18th International Conference on e-Health Networking, Applications and Services, pp. 1-3, Germany, 2016.
 15. T. McGhin, K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities", Journal of Network and Computer Applications, vol. 135, pp. 62-75, 2019.
 16. C. C. Agbo , Q. H. Mahmoud and J. M. Eklund, "Blockchain Technology in Healthcare: A Systematic Review", Healthcare, vol. 7, no. 2, article no. 56, 2019.
 17. A. A. Siyal et al., "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives", Cryptography, vol. 3, no.1, article no. 3, 2019.
 18. C. Esposito, A. Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A Panacea for Healthcare CloudBased Data Security and Privacy?", IEEE Cloud Computing, vol. 5, 2018.
 19. W. J. Gordon, and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to PatientDriven Interoperability", Computational and Structural Biotechnology Journal, vol. 16, pp. 224-230, 2018.
 20. T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in IEEE 20th International Conference on e-Health Networking, Applications and Services, pp. 1-7, Czech Republic, 2018.
 21. L. Bell, W. J. Buchanan, J. Cameron, and O. Lo, "Applications of Blockchain Within Healthcare", Blockchain in Healthcare Today, vol. 1., 2018.
- Blockchain for IoT", Sensors, vol. 19, no. 2, article no. 326, 2019.