Securing Images with Fingerprint Data using Steganography and Blockchain

S. Pramothini, Y.V.V.S. Sai Pavan, N. Harini

Abstract: ***Innovation of technology and the availability of fast Internet makes information distribution over the world easy and economical. This has attracted many adversaries who work for stealing and tampering the privacy and the works of legitimate users. Steganography and digital watermarking techniques have been continuously adopted in research for enhancing the security of data, specifically images. Recent research has shown the ability of blockchain to play an integral role in storage and distribution of medical images in a more secure fashion. With the aim of verifying the suitability of blockchains to offer an efficient and autonomous mechanism for securing images. A scheme that uses steganography to ensure confidentiality and blockchains to ensure non-repudiation is presented in this paper. Detailed experimentation brought out the ability of the proposed scheme in terms of enhancing the security compared to existing schemes in the literature.***

Key words: Blockchain, Non-repudiation, Hash, Steganography, Fingerprint

I. INTRODUCTION

With the rapid development of technology, privacy and security have become major concerns for any smartphone user. Image theft and misuse are common crimes against which one needs proper security measures. The user's photos need to be secured such that only authorized personnel can access them. Even though data sharing has increased to a great extent over the years, it adds to the existing security woes. The protection of personal images is the primary concern of the user and this paper presents a scheme that is capable of enhancing the security using steganography principles integrated with blockchain technology. Section 2 presents literature review. Section 3 presents the summary of findings justifying the need for this work. Section 4 presents the proposed scheme. Section 5 presents results and discussions. And finally Section 6 presents conclusions and scope for future work.

II. LITERATURE REVIEW

A. Fingerprint Identification

Security tokens of category inherent in users include fingerprint as one of the most common biometric traits for civil and forensic recognition process. Although other biometric traits like iris, facial scans, voice etc. are

popular, fingerprints are widely accepted because of its simplicity in usage. This simplicity factor makes fingerprint comparison algorithms to work with datasets at an ease but gives less accurate results. [4] presents a scheme to reduce the number of comparisons by using pre-filtering techniques that could be grouped under exclusive classification method and fingerprint indexing method. The authors claim that exclusive fingerprinting techniques divide the dataset into a fixed number of classes during the identification phase and as a result leads to unevenly distributed classes which are not highly efficient. On the other hand, fingerprint indexing methods were found to offer robust and efficient ways to recognize fingerprints. Reference [3] presents biometrics-based authentication methods based on symmetric hashing of the minutiae information extracted from fingerprint and using the created hash space for identifying registered prints.

B. Digital Watermarking and Steganography

Digital watermarking [6] is a technique applied to images, audio and video to facilitate copyright management, track the source of information, monitor, broadcast and detect tampering of data. This method is free of key and this is the factor which differentiates it from cryptography techniques. Watermarking techniques [7] are generally classified as fragile and robust. The former one is usually utilized to detect whether the host signal is tampered, while the latter one is used to protect the owner's legal rights and is widely used nowadays.

In contrast to cryptography that uses a symmetric or asymmetric key to encipher and decipher messages, [1] steganography is a methodology that writes hidden messages in plain sight in such a way that only intended users know the existence of the message. The original message and the embedded message generally form the cover text. For instance, a message may be hidden by using invisible ink between the visible lines of innocuous documents.

Cryptographic methods [5] are based on symmetric or asymmetric keys to guarantee confidentiality. These can be integrated with hashing and signature schemes to enhance the level of security by guaranteeing integrity and non-repudiation features. Asymmetric cryptographic algorithms like Rivest-Shamir-Adleman (RSA), Elliptic-curve cryptography (ECC) have gained popularity in the recent years for enhancing the security of applications like banking and info-sharing in social media etc.

Applying these techniques on images lead to high overheads in terms of encrypting and decrypting large amounts of data required to store even a simple image. Since the steganography [2] technique simply hides the secret message in an image, the overhead involved is comparatively less.

Revised Manuscript Received on December 30, 2018.

S. Pramothini, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India.

Y.V.V.S. Sai Pavan, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India.

N. Harini, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India.

This makes it better suitable for securing images, audio and video.

C. Blockchain

Introduction

Blockchain [8] is a technology for enhancing the integrity introduced in the recent years specifically for handling money-related transactions. The decentralized nature of Blockchain has made an attractive platform for ensuring integrity in storage mediums also. The work focuses on exploring the suitability of Blockchain in ensuring integrity in the mobile storage medium. The capability of Blockchain in terms of guaranteeing non-repudiation is also evaluated in this work with the usage of fingerprint trait encoded using steganography into the photos taken using the system camera.

A block in a blockchain [9] generally consists of a header and a body, with the header including attributes like version of the block, Merkle tree root hash, timestamp of transaction, nBits, a number used once (nonce) and parent block hash. The block version indicates the set of block validation rules to be followed. Merkle tree root hash represents the hash value of all the transactions. Timestamp saves the transaction time. nBits contains the target threshold of a valid block hash. Nonce is a 4-byte field for hash value computation. The 256-bit parent block hash points to the previous block.

The body portion of the block is composed of transactions including a transaction counter. The size of the block and the size of the transactions generally predict the maximum number of transactions that can be held in a block. Blockchains generally use public key cryptographic mechanisms for authenticating and validating transactions. Signature schemes are integrated to ensure trustworthy entries in the blockchain. In this work, the body portion of the blockchain holds the hash values computed for the captured image which has its fingerprint data hidden in it using steganography.

Digital Signature

Signature schemes [5] use asymmetric key cryptographic principles for the signing and verification processes. The participants are generally provided with a public and private key pair of which the private key is to be kept in confidentiality and this is to be used for signing the transactions. These signed transactions are verified by the recipient using the public key of the signer. Any transactions failing the verification process would be rejected by the receiver. Digital signatures could be integrated with symmetric or asymmetric cryptographic schemes to ensure confidentiality of the transaction. Digital signature algorithms like Digital Signature Algorithm (DSA),Elliptical Curve Digital Signature Algorithm (ECDSA) have gained popularity because of their small key sizes and their strength in guaranteeing message integrity and non-repudiation.

Key Characteristics of Blockchain

The key characteristics [9] of a blockchain includes, *Decentralization* which helps one in removing third-party involvement in validation, *Persistency* which ensures system integrity and non-repudiation, *Anonymity* which preserves the real identity of users and *Auditability* which enables tracking and verification of transactions.

III. SUMMARY OF FINDINGS

Image theft is a widespread problem. [11] China, France and the US are ranked first, second and third respectively with respect to the extent of digital image copyright violation. According to a 2016 survey by Berify [10], 64% of professionals and 44% of the rest claimed to have had their work stolen. Photographers and photo agencies lose hundreds of dollars due to image theft. Due to social media applications such as Instagram and Facebook, bloggers, commercial businesses and individual professionals do most of the photo-stealing. A GuardChild survey revealed that seventeen percent of the children between ages 8 and 12 surveyed received an email or message with photos that made them feel uncomfortable and only seven percent of parents were aware of this. If mobiles were equipped with a scheme ensuring non-repudiation, it would prevent real users from becoming victims. The paper presents a usable, simple framework based on blockchain and steganography to enhance the integrity and non-repudiation feature of images shared in social media. It helps the recipient verify the identity of the person who actually captured the photo.

IV. PROPOSED SYSTEM

Current systems are unable to decipher the true origins of a picture. Hence, the origin is always traced back to the phone from where the picture was taken. Unlike previous systems, the work matches the photo to a person and not a device. The existing process of sharing images through social media is depicted in Fig. 1.

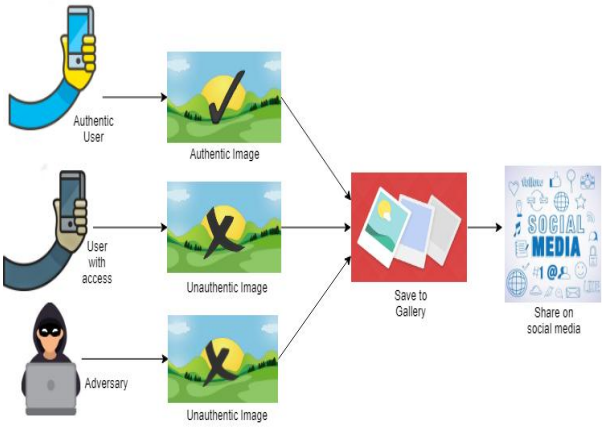

Fig. 1: Present procedure for sharing images on social media

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

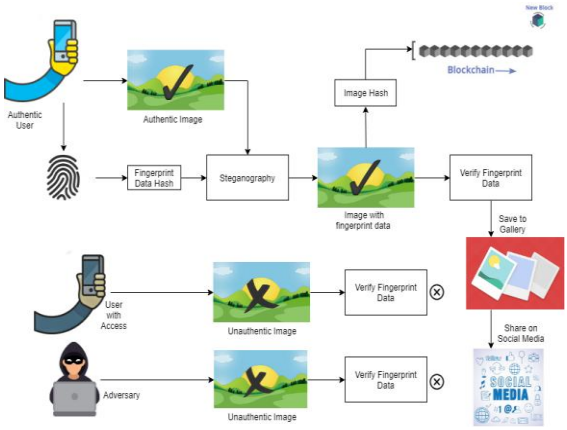

Fig. 2: Proposed scheme for sharing images on social media

In current systems, an image captured by anyone with access to the device, either an authorized user or an adversary, is saved to the gallery and can be published to social media. This violates user's security and privacy. The proposed scheme for secure sharing of image posts (Fig. 2) comprises of four phases: section A discusses the procedure for scanning the user's fingerprint, section B elaborates the methodology used for encoding the image with fingerprint data, section C discusses the phenomenon of secured indexing of image and finally section D discusses the procedure for validating the user with their fingerprint data extracted from the image.

A. Scanning the User's Fingerprint

When a user needs to capture an image, he/she will need to place their finger on the device's fingerprint scanner. The device then captures the image and records the user's fingerprint. The usage of the external fingerprint scanning device prevents the storage of the scanned fingerprint in the mobile phone. The process of capturing an image using fingerprint is illustrated in the Fig. 3.

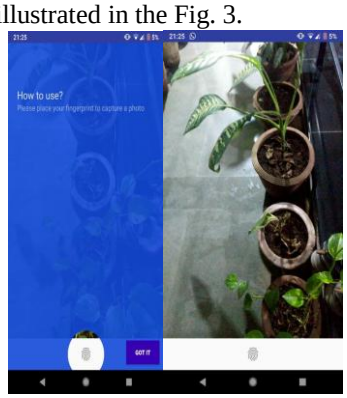

Fig. 3: Screenshots of the mobile application developed

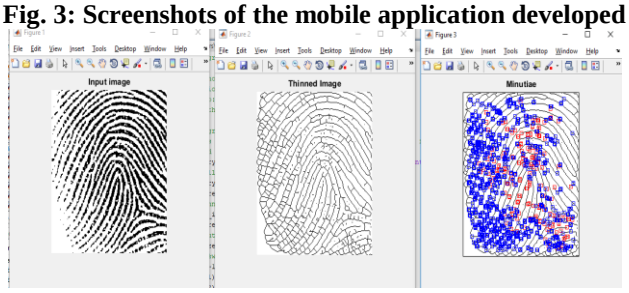

Fig. 4(a): Minutiae points of captured fingerprint

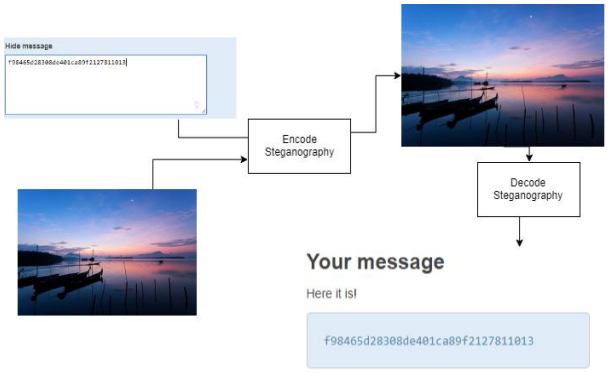

Fig. 4(b): Stepwise workflow of steganography

B. Encoding the Fingerprint Data

After the successful scanning of user's fingerprint, unique fingerprint data is generated. Attributes like minutia position and ridges bifurcation are used in calculating the fingerprint data. The generated details are used in the encoding process. Fig. 4(a). depicts the minutiae positions of fingerprint ridges. Here, encoding is done using steganography [13] where the generated unique fingerprint data [12] is embedded into the captured image. The steganography process is outlined in Fig. 4(b).

C. Secured Indexing

On the success of steganography, a hash of the encoded image is created. This hash is stored in the body of the block with the header containing hash of the previous block and is added to the blockchain [15]. In this way, one can keep track of the images taken by an authentic user.

D. Validating Image

On successful capture of the image, it is decoded for fingerprint data. If the fingerprint data obtained matches with the device owner's fingerprint, the image is saved to gallery. On account of a mismatch, the captured image is discarded without being saved to the gallery.

V. RESULTS AND DISCUSSIONS

Although the literature mentions a number of techniques [14] like cryptography, watermarking, steganography etc. for securing messages, the work has chosen steganography methodology for the reason that the existence of a hidden message is obscured from non-legitimate users. Message-Digest 5 (MD5) hash is well-suited for mobile environments because of its fast processing and small overhead. The work uses MD5 hash to obtain the hash value of the image generated from steganography which is stored in the blockchain. [16] Blockchain's non-mutable indexing property ensures non-repudiation, i.e. the authentic user cannot claim that he/she hasn't taken the picture. This can also help in ensuring security that even if an adversary was able to get a hold of user fingerprint data and embed it into image via steganography, he/she won't be able to insert image hash into the blockchain.

Fig. 5. shows the snippet of the source code implementation which reads an image and applies MD5 hash on it, after which it gets added to the blockchain.

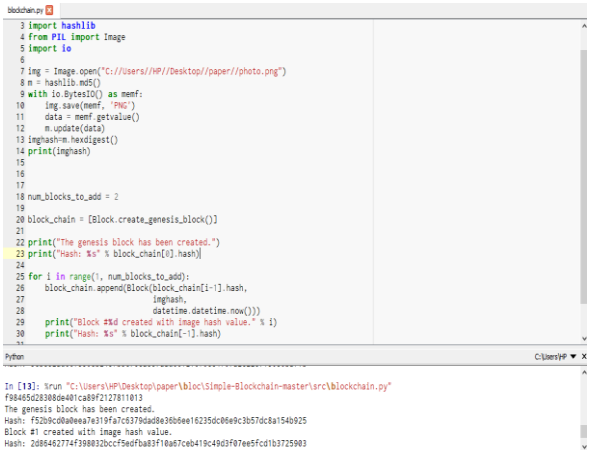

Fig. 5: Snapshot of blockchain code snippet

VI. CONCLUSION AND SCOPE FOR FUTURE

The openness of the Internet has opened new ways for invading the privacy of legitimate users by hackers and unauthorized users. Literature presents many techniques to solve this problem like steganography, digital watermarking, cryptography etc. The paper presents a hybrid security scheme that uses steganography combined with blockchain technology to enhance the security of image posts shared in the social media.

Presently, Android operating systems use Trusted Execution Environment(TEE) to store recorded fingerprints. The TEE is a secure, isolated execution environment which cannot be accessed by the users or any apps. Hence, one can only authenticate the recorded fingerprints and not retrieve or modify them. In order to capture user fingerprints, one can use external fingerprint scanners compatible with Android Software Development Kit(SDK). A feature enabling the recording of fingerprints can be expected from Android in the near future.

Ideally, blockchain is stored in a cloud database as it takes up huge volumes of storage space and requires large amounts of processing. Cloud storage has its own disadvantages related to data ownership and security. These security lapses can be overcome in the future by using optimized techniques to store the blockchain in the owner's device directly.

REFERENCES

1. S. Kaur, S. Bansal and R. K. Bansal, "Steganography and classification of image steganography techniques," *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2014, pp. 870-875.
2. A. A. J. Altaay, S. B. Sahib and M. Zamani, "An Introduction to Image Steganography Techniques," *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, Kuala Lumpur, 2012, pp. 122-126.
3. Tulyakov Sergey, Farooq Faisal, Govindaraju Venu, "Symmetric Hash Functions for Fingerprint Minutiae", Springer Berlin Heidelberg ,Berlin, Heidelberg.
4. R. Cappelli, M. Ferrara and D. Maltoni, "Fingerprint Indexing Based on Minutia Cylinder-Code," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 5, pp. 1051-1057, May 2011.
5. Dr T.R Padmanabhan, N.Harini and Dr.C.K.Shyamala, "Cryptography and security", WileyIndia, FirstEdition, 2011
6. Cox, Ingemar & Miller, Matthew & Bloom, Jeffrey & Fridrich, Jessica & Kalker, Ton, "Digital Watermarking and Steganography",
7. Yafeng Zhou and W. W. Y. Ng, "A study of influence between digital watermarking and steganography," *2013 International Conference on Wavelet Analysis and Pattern Recognition*, Tianjin, 2013, pp. 49-55
8. doi: 10.1109/ICWAPR.2013.6599291
9. L. S. Sankar, Sindhu, M., and Sethumadhavan, M., "Survey of consensus protocols on blockchain applications", in 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017, 2017
10. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, 2017, pp. 557-564
11. Rose Leaden, "A Snapshot of Online Image Theft", Entrepreneur India (2018) , Berify, https://www.entrepreneur.com/article/309876
12. Andrea Feustel, "Image Theft Ranking", Copy Track (2017), https://www.copytrack.com/image-theft-ranking
13. Sergey Tulyakov, Faisal Farooq, Praveer Mansukhani, Venu Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems",*Pattern Recognition* Letters, *Volume 28, Issue 16, 2007*, Pages 2427-2436, ISSN 0167-8655
14. S. Anjana and Amritha, P. P., "A Novel Method for Secure Image Steganography", in *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems: Proceedings of ICAEES 2014*, Volume 1, P. L. Suresh, Dash, S. Subhransu, and Panigrahi, K. Bijaya New Delhi: Springer India, 2015, pp. 151–158
15. Abira Dasgupta ,Rajesh kumar tiwari ,Arup paul, "Digital watermarking and Steganography Techniques:A Technical overview", *International Journal of Computer Engineering and Applications*, Special Edition, www.ijcea.com ISSN 2321-3469
16. H. G. Do and W. K. Ng, "Blockchain-Based System for Secure Data Storage with Private Keyword Search," *2017 IEEE World Congress on Services (SERVICES)*, Honolulu, HI, 2017, pp. 90-93. doi: 10.1109/SERVICES.2017.23
17. W. Pourmajidi and A. Miranskyy, "Logchain: Blockchain-Assisted Log Storage," *2018 IEEE 11th International Conference on Cloud Computing* (CLOUD), San Francisco, CA, 2018, pp. 978-982. doi: 10.1109/CLOUD.2018.00150

S. Pramothini is a B.Tech student currently pursuing Computer Science and Engineering degree at Amrita School of Engineering, Coimbatore. Her research interests include image processing and indoor localization.

Y.V.V.S. Sai Pavan is an undergraduate student at Amrita School of Engineering, Coimbatore and will be graduating in 2019 with a B.Tech degree in Computer Science and Engineering. He has a strong interest in the field of Cryptography and Information Security.

Dr.N. Harini currently serves as Assistant Professor in the Department of Computer Science and Engineering at Amrita School of Engineering, Coimbatore Campus. Her Qualifications are Ph.D, MCA, MPhil and her primary area of research is Security.