ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 10, October 2024

Protecting Ownership And Privacy In Social Media

[1] Anisha. M, [2]Angelin Rosy.M
[1] Student: Department Of Mca, Er Perumal Manimekalai College Of Engineering(Autonomous) ,Hosur, Tamil Nadu, India
[2] Assistant Professor, Department Of Mca, Er Perumal Manimekalai College Of Engineering(Autonomous),Hosur, Tamil Nadu, India

Abstract: ***Social networks are increasingly becoming essential for users to connect and share information, whether for personal, professional, or recreational purposes. A rising trend is the daily sharing of photos on online Social Network Platforms (SNPs), where the privacy of these photos is often protected by security mechanisms. However, the effectiveness of these mechanisms diminishes once the photos are shared across different platforms. This project proposes a block chain-based secure photo-sharing framework that enhances photo dissemination control across heterogeneous social networks.***
Unlike traditional security mechanisms that operate on centralized servers, this framework uses block chain technology to achieve a consistent consensus on photo-sharing control through smart contract protocols. The proposed protocols ensure platform-free dissemination trees for every image, giving users complete control over their sharing preferences while maintaining privacy. Additionally, this system introduces a dynamic privacy policy generation algorithm, which maximizes the flexibility of re-posters without compromising the privacy of original owners.

I. INTRODUCTION

With today's ubiquitous internet service, digital images can be conveniently downloaded and shared through social networking services (SNS) such as Facebook, Snapchat, Twitter, etc. Therefore, there are vital needs to provide some mechanisms to manage – originally was 'protection' the vast number of originals images. Information hiding (i.e., data embedding) is the process of inserting external information (e.g., ownership information and secret message) into a medium. It is one of the possible solutions to serve the aforementioned needs. Fig. 1 illustrates the general framework during the data embedding process. Data is inserted into the cover image with a secret key to produce an output image with embedded data, while aiming to achieve high perceptual image quality, large embedding capacity, and strong resistance to attacks.

II. SOFTWARE ANALYSIS

- Server Side : Python 3.7.4(64-bit) or (32-bit)
- Client Side : HTML, CSS, Bootstrap
- IDE : Flask 1.1.1
- Back end : MySQL 5.
- Server : Wampserver 2i
- OS : Windows 10 64 –bit or Ubuntu 18.04 LTS "Bionic Beaver"

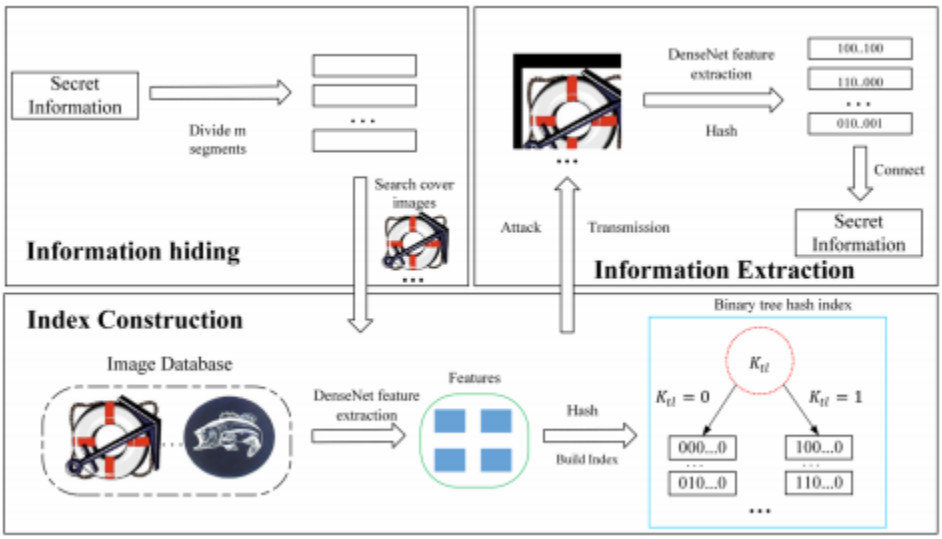

Fig1

PYTHON 3.7.4:

Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This tutorial gives enough understanding on Python programming language.

NUMPY:

NumPy, which stands for Numerical Python, is a library consisting of multidimensional array objects and a collection of routines for processing those arrays. Using NumPy, mathematical and logical operations on arrays can be performed.

MATPLOTLIB:

Matplotlib is a comprehensive library for creating static, animated, and interactive visualizations in Python. Matplotlib makes easy things easy and hard things possible.

Matplotlib is a plotting library for the Python programming language and its numerical mathematics extension NumPy. It provides an object-oriented API for embedding plots into applications using general-purpose GUI toolkits like Tkinter, wxPython, Qt, or GTK.

SEABORN:

Seaborn is a library for making statistical graphics in Python. It builds on top of matplotlib and integrates closely with pandas data structures. Visualization is the central part of Seaborn which helps in exploration and understanding of data.

MYSQL:

MySQL tutorial provides basic and advanced concepts of MySQL. Our MySQL tutorial is designed for beginners and professionals. MySQL is a relational database management system based on the Structured Query Language, which is the popular language for accessing and managing the records in the database. MySQL is open-source and free software under the GNU license. It is supported by Oracle Company. MySQL database that provides for how to manage database and to manipulate data with the help of various SQL queries. These queries are: insert records, update records, delete records, select records, create tables, drop tables, etc. There are also given MySQL interview questions to help you better understand the MySQL database.

III. EXISTING SYSTEM

Firstly, the cover image is segmented into a number of fragments. Secondly, in order to use the MSB of cover image to represent the secret information, the average intensity of each fragment is calculated. Thirdly, a one-to-one mapping between the MSB of the image fragment and the secret information is established using the mapping sequence (denote as Kr), decided by the sender and the receiver in advance. This process produces a mapping flag (denote as K f), which is sent by the sender along with the step go image.

In order to improve the robustness against geometric attacks, we propose a coverless image steganography method based on multi-object recognition. In this scheme, we firstly use Faster RCNN to detect objects in the image data set, establish a mapping dictionary between object labels and binary sequence. Then we propose a novel mapping rule based on the filtered robust object labels for sequence generation. Therefore, an image can generate robust binary sequence through multi-objects recognition. In the transmission process, the transmitted image has not been modified, so our method can fundamentally resist steganalysis tools and avoid the attacker's suspicions.

IV. MODULES

SOCIAL NETWORKING WEB APP
PHOTO CHAIN INYTEGRARTION
SN USER DASHBOARD
PHOTO PRIVACY
PHOTO BLUR
PHOTO PRIVACY VIOLATION
PHOTO INTEGRTY VERIFICATION
PERFORMNACE ANALYSIS

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 10, October 2024

ARCHITECTURE DIAGRAM

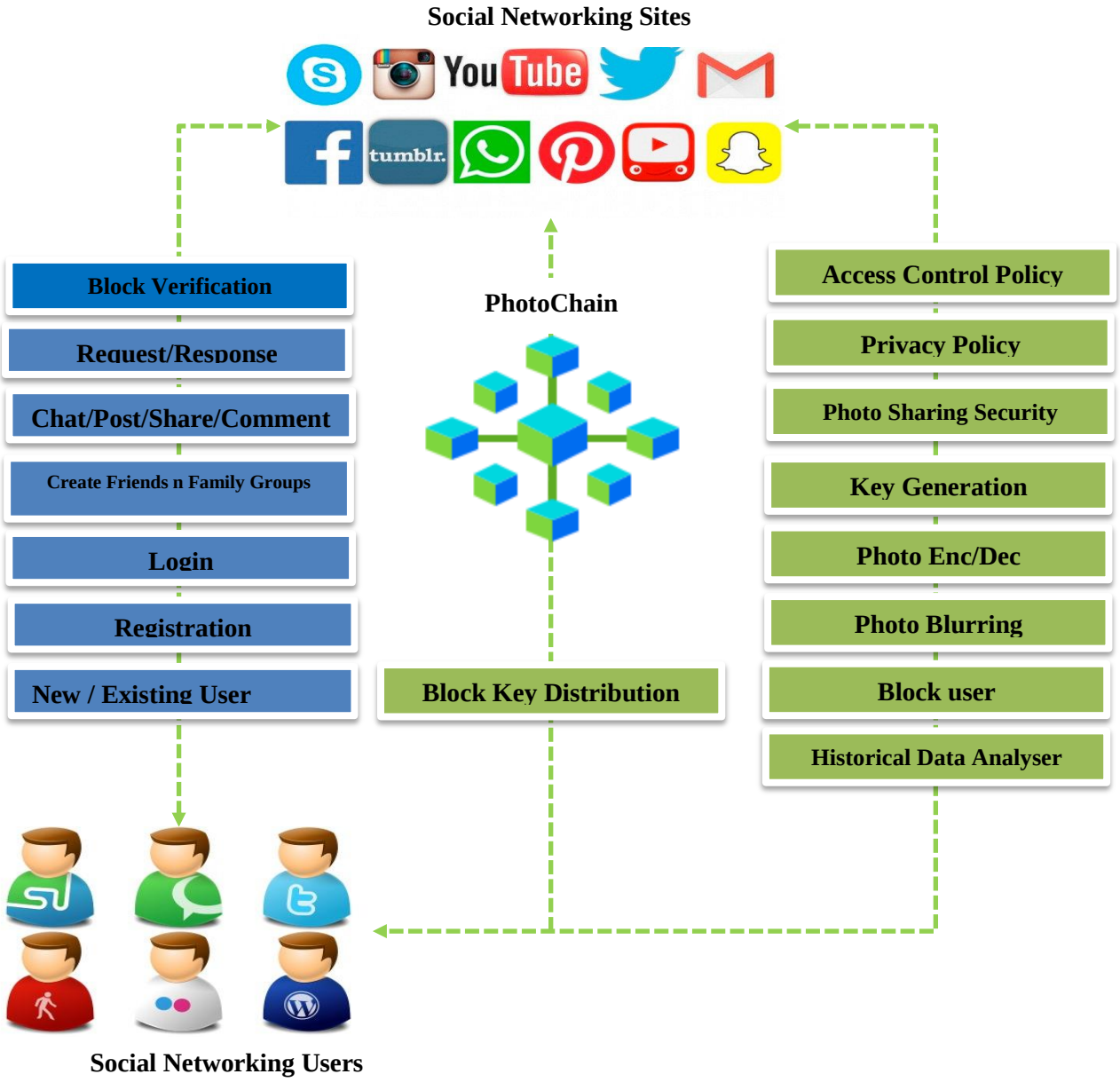

Fig.2. ARCHITECTURE DIAGRAM

V. RESULT

Protecting ownership and privacy in social media involves implementing strategies, technologies, and practices that ensure user data remains private and that content ownership rights are respected. Here are some key results and approaches:

End-to-end encryption ensures that user communications and data are secure from unauthorized access Blockchain technology can establish immutable ownership records for user-generated content . Used to protect individual data while allowing aggregate analysis for insights.

Digital watermarking for photos and videos helps prove ownership of content . Compliance with GDPR, CCPA, and other regulations ensures platforms protect user data and respect privacy rights. Content Ownership Agreements: Transparent terms of service that clarify user ownership and licensing rights.

VI. CONCLUSION

This project proposed a new idea for CIH. Driven by secret information and constrained by attribute labels, it directly generates anime character with high quality to transmit secret information. Compared with the current cover selection methods, proposed method has a great improvement in capacity. However, there is a gap in robustness compared with the current robust coverless information hiding methods.

The next step is to improve the robustness of the method by optimizing the generation model. This paper provides a more practical solution for the development of coverless information hiding, that is, to express secret information in the process of generating target images according to attributes, which has certain guiding significance for the development of coverless information hiding.

REFERENCE

[1] Prema, G.; Natarajan, S., "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application," Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.727,730, 21-22 Feb. 2013. [2] Nickfarjam, A.M.; Azimifar, Z., "Image steganography based on pixel ranking and Particle Swarm Optimization," Artificial Intelligence and Signal Processing (AISP), 2012 16th CSI International Symposium on , vol., no., pp.360,363, 2-3 May 2012.
[3] Sanchez, A.; Conci, A.; Zeljkovic, E.; Behlilovic, N.; Karahodzic, V., "A new approach to relatively short message steganography," Telecommunications (BIHTEL), 2012 IX International Symposium on , vol., no., pp.1,4, 25-27 Oct. 2012.
[4] Qiangfu Zhao; Akatsuka, M.; Cheng-Hsiung Hsieh, "Generating facial images for steganography based on IGA and image morphing," Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on , vol., no., pp.364,369, 14-17 Oct. 2012.
[5] Khosravi, M.; Soleymanpour-Moghaddam, S.; Mahyabadi, M., "Improved pair-wise LSB matching steganography with a new evaluating system," Telecommunications (IST), 2012 Sixth International Symposium on , vol., no., pp.982,986, 6-8 Nov. 2012.
[6] Brazil, A.L.; Sanchez, A.; Conci, A.; Behlilovic, N., "Hybridizing genetic algorithms and path relinking for steganography," ELMAR, 2011 Proceedings , vol., no., pp.285,288, 14-16 Sept. 2011.
[7] Bhowal, K.; Sarkar, D.; Biswas, S.; Sarkar, P.P., "Secured image transmission with GA based Audio Steganography," India Conference (INDICON), 2011 Annual IEEE , vol., no., pp.1,4, 16-18 Dec. 2011.
[8] Mandal, J.K.; Khamrui, A., "A Genetic Algorithm based steganography in frequency domain (GASFD)," Communication and Industrial Application (ICCIA), 2011 International Conference on , vol., no., pp.1,4, 26-28 Dec. 2011.
[9] W. Tang, S. Tan, B. Li, and J. Huang, ‘‘Automatic steganographic distortion learning using a generative adversarial network,’’ IEEE Signal Process. Lett., vol. 24, no. 10, pp. 1547–1551, Oct. 2017.
[10] H. Naito and Q. Zhao, ‘‘A new steganography method based on generative adversarial networks,’’ in Proc. IEEE 10th Int. Conf. Awareness Sci. Technol. (iCAST), Oct. 2019, pp.