iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35662

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Prevention of Clone Attack in Online Social Media Integrating Secure Data Transmission

Abishek Kashayap. S[1], Anurag S. S. S. M[2]
[1, 2]*Department of Computer Science and Engineering, St. Joseph's Institute of Technology, OMR, Chennai-600119, India*

Abstract — Social networking is becoming so essential nowadays and is playing a bigger role in every man's life for sharing information and knowledge. Also social network is used to see the everyday activities, photos, videos, political agendas and propagandas. Therefore, it is now becoming an important tool to stay updated in this dynamic world. With large chunks of data being generated every second, there is a growing concern about Data protection and user privacy in the Social media network. One of the major concerns being, 'Fake Users' - misusing the authorized user's information like photos and videos without the authorized user's permission and disguising oneself as a legitimate user. In our contemporary world, many fake profiles are being created for fraudulent activities like money making, malware / virus / Trojan distribution to use user data, especially with malicious intent. In this paper Java static watermarking is proposed. Java static watermark is used in our social media website in order to associate each user's footprint with respect to their unique ID, eliminating the crux of fake users. It is also very evident to say that data present on the cloud is no less prone to cyber-attacks. In this paper, integration of steganography methods for protection of sensitive data on the public cloud server is also proposed to validate its viability and its increased security. The Algorithms used ensure the individual information is kept secret and transmitted in a secure manner with user privacy preserving.

Keywords— Java Static Watermark, Steganography, Discrete Wave Transform (DWT), Discrete Cosine Transform (DCT), Social Networking website, Clone Attack, Data Privacy, Automated Scanning, Intrusion Detection System

I. INTRODUCTION

Millions of active users all around the world are using online social networks, such as Facebook, Twitter, Tumbler and LinkedIn. It makes it effortless to misuse user's information and do identity cloning attacks to form fake profiles. In this proposed system, data hiding techniques are used to hide some unique information in profile pictures in order to detect botnets and fake profiles. This paper presents a classification and analysis of detection mechanisms of clone attacks on online social networks, based on attribute similarity, friend network similarity, and profile analysis for a time interval and record of Internet Protocol sequences. Discrete wavelet transform algorithm is used for data hiding. Thus this would prevent the clone attack**s** and provide complete user data privacy. Also when users upload the profile picture or photos it would be watermarked and updated. For watermarking, Java static watermarking systems and algorithms are used. Any fake user updating the same profile picture can be detected and their respective IP would be tracked and blocked. Also for secure image transmission, we use Discrete Wavelet Transform (DWT) for data hiding / steganography on cloud combined with Discrete Cosine Transform (DCT) for image compression. For our experimental analysis, we are going to design and develop a cloud based web application invoking Java static watermarking (clone attack), data hiding and image compression.

A hybrid image authentication watermark can be obtained as a combination of fragile and a robust watermark. The fragile watermark has the advantages that it has good localization and security properties. The hybrid watermark can be used to precisely identify changes as well as distinguish malicious tamper from simple operations. The authentication can be done without accessing any information about the original image. Effective Hybrid Digital Watermarking Scheme Using Direct Sequence-Spread Spectrum Method – in this scheme, a watermark image is produced using the personal ID of the copywriter which is inserted into the original images and the watermark image is detected. It is an extension of the spread spectrum watermarking scheme which combines key with logo method. Binary image is used as watermark image, and the degradation of image quality between original image and watermarked image is applied to confirm required invisibility in watermark system and watermark robustness is applied to protect an attack from the outside are analysed using the values of PSNR of the watermark image.

The DCT transforms a signal from a spatial representation into a frequency representation. Lower frequencies are more obvious in an image than higher frequency so if we transform an image into its frequency component and throw away a lot of higher frequency coefficients, we can reduce the amount of data needed to describe the image without sacrificing too much image quality. The discrete cosine transform (DCT) is closely related to the discrete Fourier transform.

Recent researchers on secure digital watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and robustness of a watermarking scheme. In this approach, watermark is created from the content of the host image and discrete wavelet transform (DWT) is used for embedding watermarks, since it is an excellent time frequency analysis method which can be adapted well for extracting the information content of the image.

Wang et al. adopt a key dependent wavelet transform. To take advantage of the localization and multi-resolution property of the wavelet transform, Wang and Lin proposed a wavelet tree based watermarking algorithm. In this approach, the host image is transformed into wavelet coefficients using a discrete-time wavelet transform (DTWT). The watermark is embedded in the wavelet coefficients which are grouped into super trees. Each watermark bit is embedded using two supertrees. Depending on the value of the watermark bit, one of the super trees is quantized with respect to a quantization index in such a way that the two supertrees exhibit a large enough statistical difference, which can be extracted for obtaining a decision.

As each watermark bit is embedded in various frequency bands and the information of the watermark bit is spread throughout large spatial regions,

Therefore, the watermarking technique is robust to attacks in both frequency and time domains. This technique is useful for removal of high-pass details in JPEG compression and robust to time domain attacks such as pixel shifting and rotation.

In addition to copyright protection, the proposed watermarking scheme can also be applied to data hiding or image authentication.

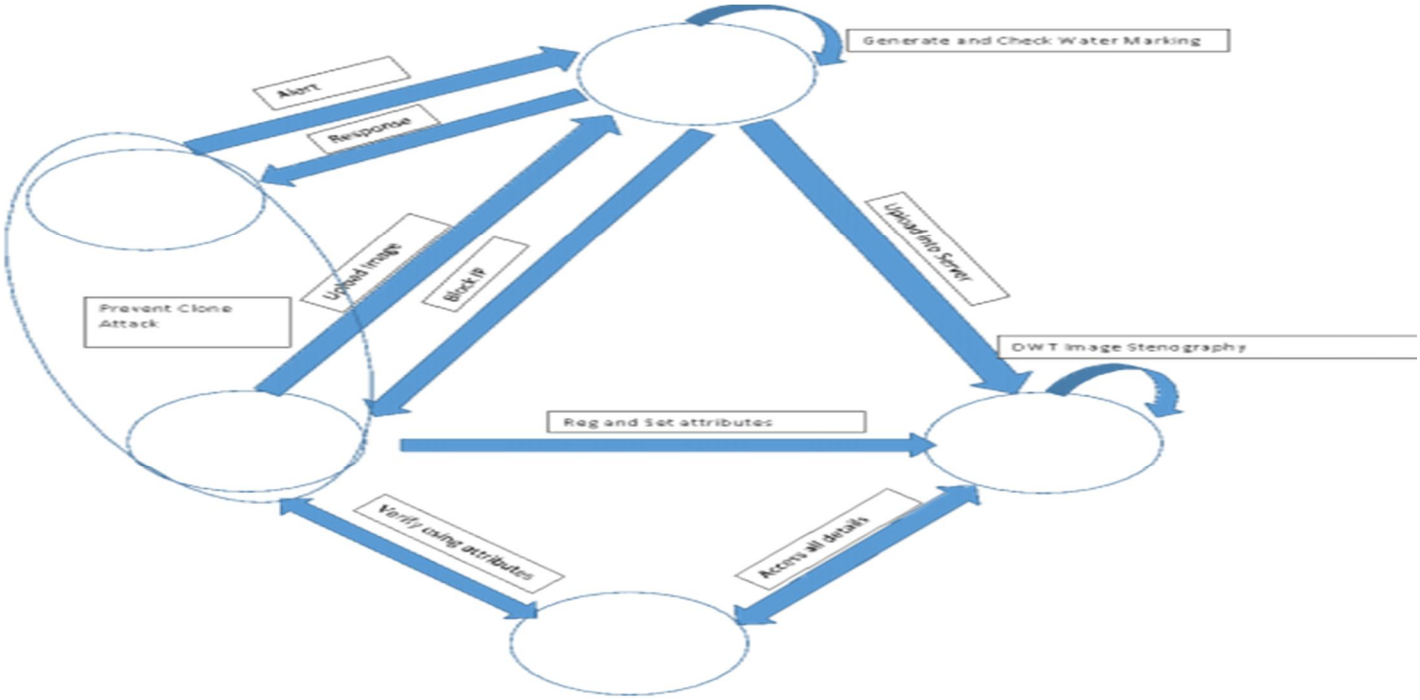


Figure 1: Architecture diagram for Prevention of Clone Attack in Online Social Media Integrating Secured Data Transmission

II. EXISTING SYSTEM

Fake accounts are categorized into what Facebook calls as duplicate accounts and false accounts. A duplicate account refers to an account maintained by a user in addition to his/her principal account. False accounts are further broken down into two categories: user-misclassified accounts and undesirable accounts. User-misclassified accounts represent the personal profiles created by users for a business, organization, or nonhuman entity such as a pet (Facebook's terms of service permits such entities as a Page rather than a personal profile). On the other hand, undesirable accounts are the user profiles that are intended to be used for purposes that violate Facebook's terms of service, such as spamming. According to an internal review by Facebook on a limited sample of its accounts, approximately 4.3% to 7.9% of Facebook's monthly active users represented duplicate accounts in 2013. In the same year, the number of user misclassified accounts were estimated to be approximately 0.8% to 2.1% of the MAUs, while the undesirable accounts were estimated to be approximately between 0.4% and 1.2% of MAUs. Such estimates rely on judgments based on identifying names appearing to be fake or other inauthentic behavior. There is currently no automated mechanism used to identify fake profiles or duplicate profiles rather than manually confirming by cross verifying them.

Disadvantages

- In the existing system there is no security for profile pictures. This vulnerability is on Facebook as well. User profile pictures are misused for creating a fake profile.
- In the existing system there is no effective secure transmission of images. Existing applications use Huffman coding algorithms for image data hiding.

III.PROPOSED SYSTEM

Detection and identifying fake profiles and botnets in social networks are restricted to the user's report and just subsequent to a number of reports for a particular user; the system will check the validation of the user.

In the proposed approach, Steganography techniques and methods will be used to detect and identify such fake profiles. In this method, at any time a user uploads his/her pictures, some exclusive and useful information such as email or username and also date of upload would be attached to pictures by means of watermarking methods. Accordingly, in future, if somebody else saves that picture and attempts to create a fake profile with stolen data, the system is able to automatically detect this deception and fraud and would prevent and protect the fake user from any additional positive action. Our proposed system invokes discrete wavelet transform algorithms for data hiding. Thus this would prevent the clone attacks and provide complete user data privacy preserving.Also when users upload the profile picture or photos it would be watermarked and updated. For watermarking techniques Java static watermarking systems and algorithms are used. Any fake users updating the same profile picture can be detected and their respective IP would be tracked and blocked. Also for secure image transmission, we used Discrete Wavelet Transform (DWT) for data hiding / steganography and Discrete Cosine Transform (DCT) for image compression. For our experimental analysis, we are going to design and develop a cloud based web application invoking Java static watermarking (clone attack), data hiding and image compression.

Advantages:

- User identity is secured.
- Clone attack would be prevented effectively in our proposed system.
- User can securely transmit the images from the user side to cloud using discrete wavelet transform.
- Clone attack is effectively prevented using new architecture involving java static watermarking technique.

IV.METHODOLOGY

A. Java Static Watermarking

Watermarking is the process of hiding digital information in a carrier signal. In this method, at any time a user uploads his/her pictures, some exclusive and useful information such as email or username and also date of upload would be attached to pictures by means of watermarking methods. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied pictures or media, respective IP would be tracked and blocked.

B. Image Steganography (DWT)

Steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography is a technique of hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.

The discrete wavelet transform is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules.

We use discrete wavelet transform algorithms for data hiding. Thus this would prevent the clone attacks and provide complete user data privacy preserving. Also when users upload the profile picture or photos it would be watermarked and updated. Steganography is the hiding of a secret message within an ordinary message.

Figure. 2 : This image represents how DWT algorithm gets applied on Rows and Columns of an Image

DWT ALGORITHM:
Step 1: Read Image.
Step 2: Select cover Frame.
Step 3: Convert to any single Plane process.
Step 4: For that Plane convert to DWT Process.
Step 5: Select Secret image.
Step 7: Embed that Secret image with the input image.
Step 8: Write a STEGO frame.
Step 9: Reconstruct image.
Step 10: Read the STEGO Frame.
Step 11: STEGO Frame Is Broken into image and cover Frame.
Step 12: Calculate each pixel of STEGO Frame.
Step 13: Retrieve bits and convert each 8 bit into one character.
Step 14: Extract the Secret image

C. Image Compression (DCT)
Discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high frequency components can be discarded), to spectral for the numerical solution of partial differential equations.
The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample.
JPEG Process Steps for color images:
This section presents jpeg compression steps.
Step 01: An RGB to YCbCr color space conversion (colour specification)
Step 02: Original image is divided into blocks of 8 x 8.
Step 03: The pixel values within each block range from [-128 to 127] but pixel values of a black and white image range from [0-255] so, each block is shifted from [0-255] to [-128 to 127].
Step 04: The DCT works from left to right, top to bottom thereby it is applied to each block.
Step 05: Each block is compressed through quantization.
Step 06: Quantized matrix is entropy encoded.
Step 07: Compressed image is reconstructed through a reverse process. This process uses the inverse Discrete Cosine Transform (IDCT).
DCT has been used for image compression after applying the steganography algorithm - which increases the size of the file to a large extent. In order to bring the size of the file to its original terms we use DCT.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

D. Intrusion Detection System

An intrusion detection system (IDS) is a software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms. In this method, the system will automatically check the right and privilege of the user and ownership of uploaded files. Subsequently to checking the uploaded file, if the

system finds the existence of watermark, it will send an announcement and a notification to the owner of original content and prevent users from re-uploading.

E. Verification Alert

If the system finds the existence of a watermark, it will send an announcement and a notification to the owner of original content and prevent User from re uploading. Fake users updating the same profile picture can be detected and their respective IPs will be blocked.

F. Cloud Storage

Public cloud storage is a storage-as-a-service model that enables individuals and organizations alike to store, edit and manage data. This type of storage exists on a remote cloud server and is accessible over the internet under a subscription-based utility billing method where the users pay only for the storage capacity being used.

CloudMe is the public cloud service that we used to experiment our image steganography techniques. In this we are storing images where steganography has been used so the system will hit the cloud to verify the ID for the specific user and verify it. Images that have been compressed after the steganography are also stored in the cloud.

V. RESULTS AND DISCUSSION

A. Watermark Implementation

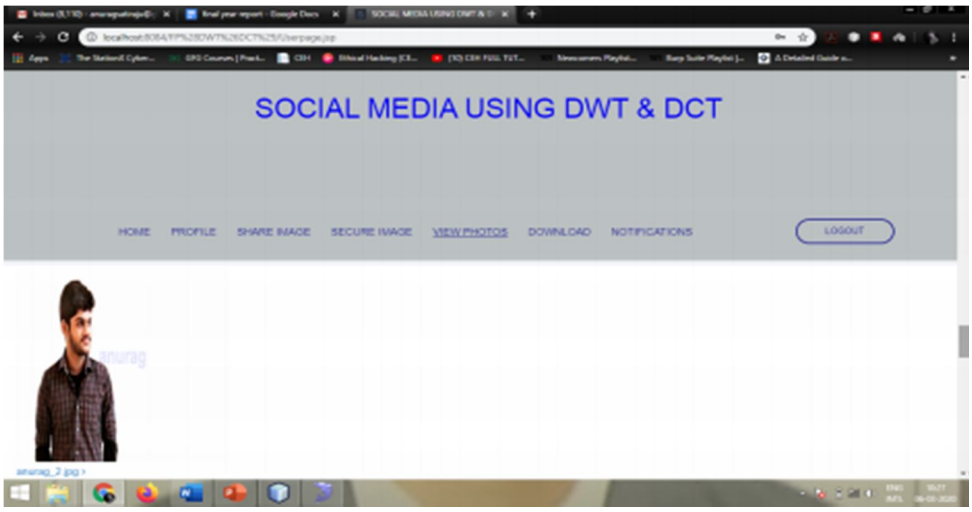


Figure 3: User Profile page for the application Prevention of Clone Attack in Online Integrating Secured Data Transmission

In above figure 2.0, It shows the profile page of the user Anurag who has been logged-in in the application using his username and password which he gave in the registration page for registering his account in the application. Where the login page and the registration page is been designed in HTML, CSS the form validation is done using JAVA where the it hits the server which is having the Database which is been created using MySQL. When user is being validated and been logged in he can now share his favourite photos in the forum to show to his friends. When, the user Anurag uploads a photo it gets uploaded with a watermark on that picture using java static watermarking.

B. Intrusion Detection System

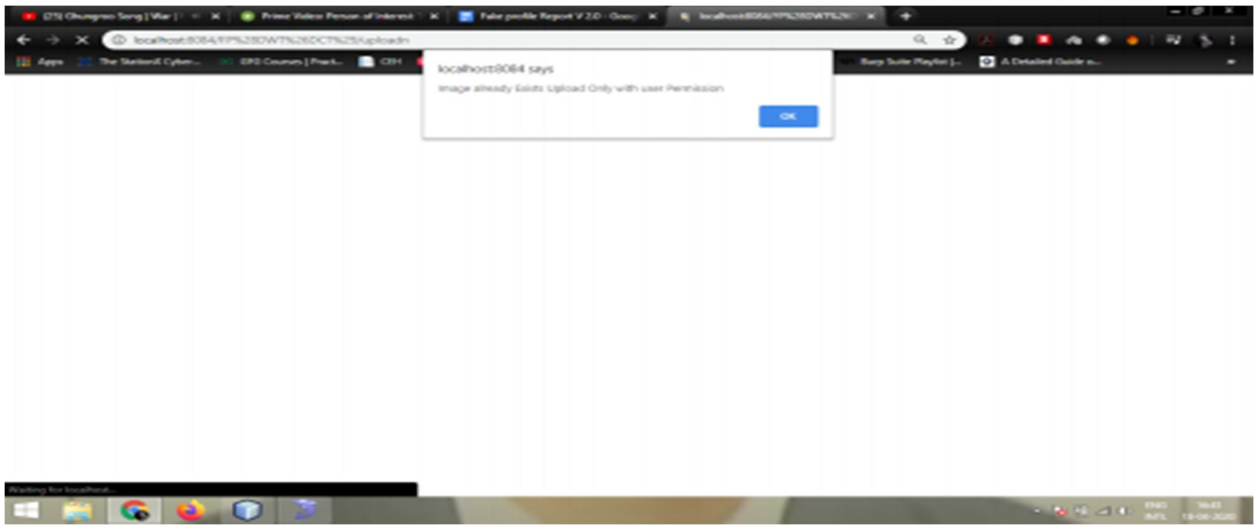


Figure 4: Notification Page for the application Prevention of Clone Attack in Online Integrating Secured Data Transmission

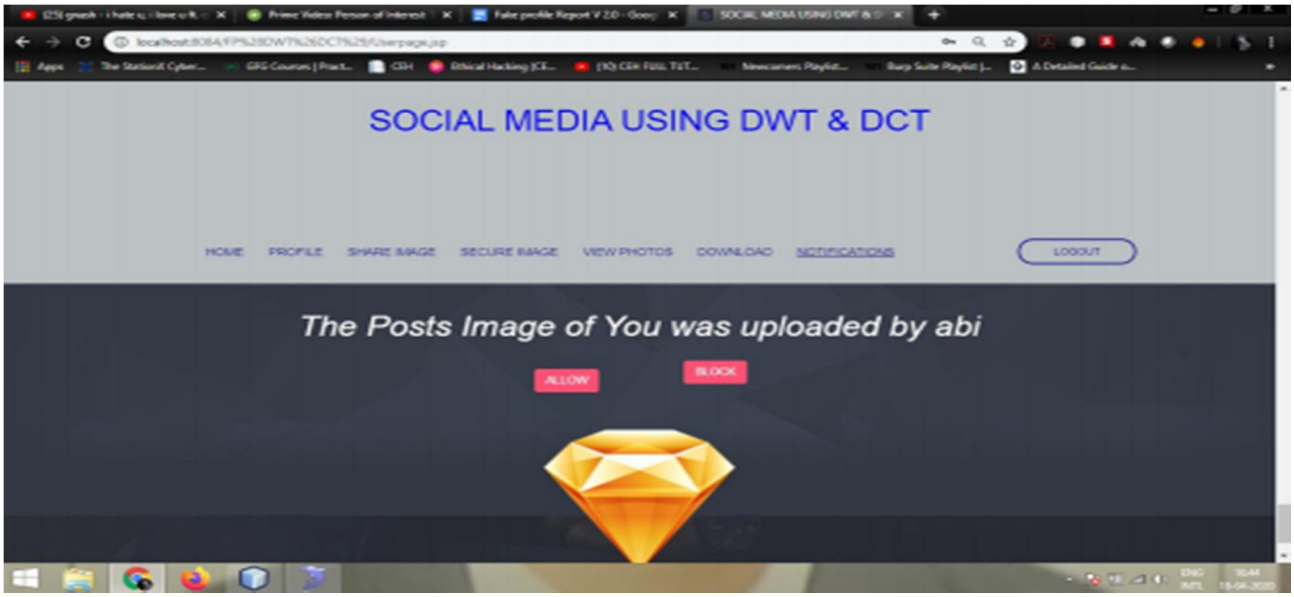


Figure 5: Intrusion Detection System for the application Prevention of Clone Attack in Online Integrating Secured Data Transmission

According to Figure 03, The message that has been popped out is the alert notification that a user will get when another user tries to upload a another users image in the application. Only if a user gives permission to upload a image the other user can upload his image. In this module the watermarking plays its role where we will have a unique watermark for each and every user which is been mapped to his user id and user name os in this Figure 6.4, the user B is trying to upload user A image from his profile where user A image has a unique watermark that is been mapped to his username as the user B is uploading user A image our application will find that it is user A image from the watermark that is present in that image. As, the application has found its user A image the user B can't able to upload without user A's permission.

Figure 04 shows us the Intrusion detection module in which a new user B has uploaded a image of user A from his account where user A gets an alert in his profile page whether to allow that user to upload the user or to block that user. If, user A clicks ALLOW user B can able to post user A's image if he clicks BLOCK user B IP and his account will be blocked.

C. Steganography Images

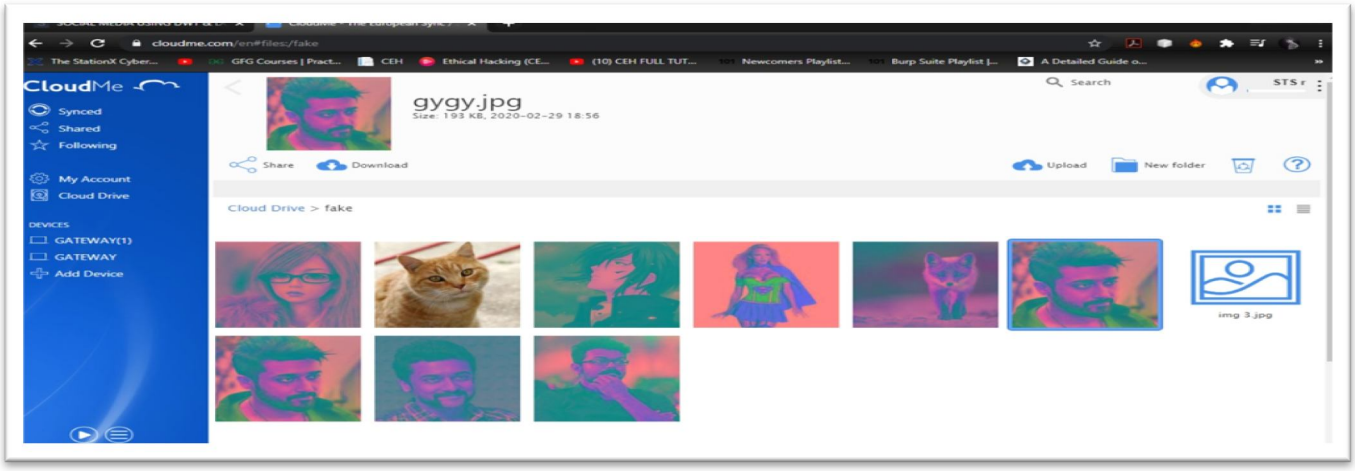


Figure 6: Steganography Images that are stored in Cloud

VI. CONCLUSION

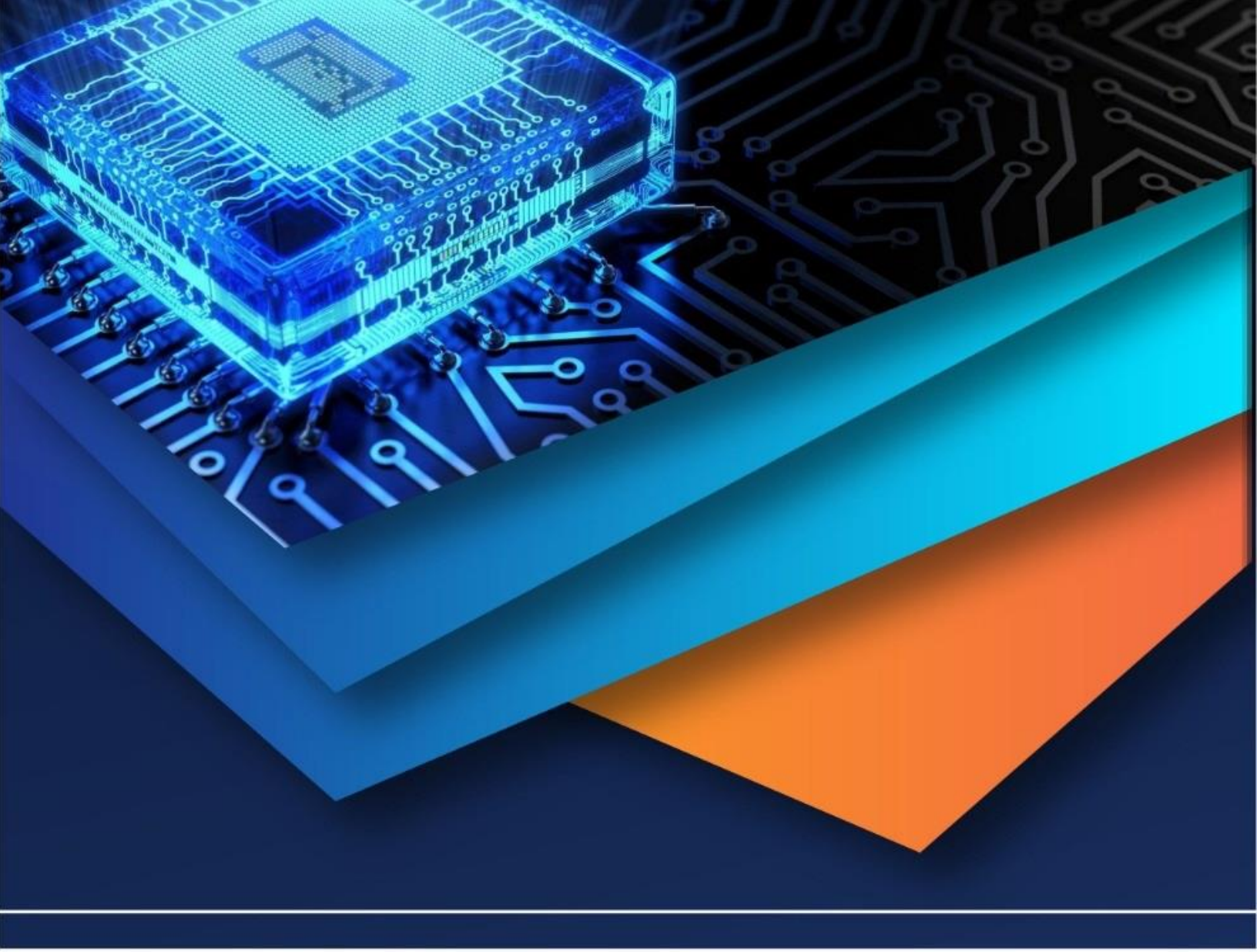
This Project presents a brief knowledge about the attacks and defence mechanisms which are prominent on Online Social networks. It also explains the work which had been performed in the field of detecting and preventing clone profiles and secure transmission of images from sender to receiver

VII. ACKNOWLEDGMENT

I would like to thank Mrs. Abirami Mani, Business Data Analyst, Telia, Sweden for helping us in collecting all data and to work on this project. Her input and kindly help were very useful in completion of this project.

REFERENCES

[1] Nielsen, Social Networks and Blogs, 4th Most Popular Online Activity, Nielsen Online Report, 2009..
[2] Boyd, D and Ellison, NB, Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, 13, 2 (2007).
[3] Stolen Facebook Accounts for Sale, http://tinyurl.com/25cngas,2010.
[4] Personal communication with the Manager of User Support and the Product Manager of the Core and Community Management teams in Tuenti, 2011.
[5] Fake Accounts in Facebook - How to Counter it, http://tinyurl.com/5w6un9u, 2010.
[6] Why the Number of People Creating Fake Accounts and Using Second Identity on Facebook are Increasing, http://tinyurl.com/3uwq75x, 2010.
[7] Guardian, Twitter Hoaxer Comes Clean And Says: I Did It To Expose Weak Media, Guardian, 2012.
[8] Post, W, Twitter Hoaxer Tommaso De Benedetti Comes Clean, Washington Post, 2012..
[9] Salon, the Fake Facebook Profile I Could Not Get Removed, Salon.com, 2012.
[10] Roberts, S, Fake Facebook Friends - People Behaving Badly, YouTube, 2012..
[11] Desai, V.H, Steganography, Cryptography, Watermarking: A Comparative Study, Journal of Global Research in Computer Science, Vol.3, No.12, Dec 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY