International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

PROTECTING FACEBOOK ACCOUNT FROM MALICIOUS ATTACKING APPLICATIONS

Sandhya Dayalan[1], M.S.Vinmathi[2]

[1]Student of Computer Science and Engineering Department, Panimalar Engineering College, Tamil Nadu, India

[2]Associate Professor of Computer Science and Engineering Department, Panimalar Engineering College, Tamil Nadu, India

---

Abstract –*This paper introduces a novel rank-based strategy for picture watermarking. In the watermark implanting process, the host picture is separated into pieces, trailed by 2-D discrete cosine change (DCT). For each picture obstruct, a mystery key is utilized to arbitrarily choose an arrangement of DCT coefficients appropriate for watermark inserting. Watermark bits are embedded into a picture hinder by changing the arrangement of DCT coefficients utilizing a rank-based installing standard. In the watermark discovery prepare, the comparing recognition lattices are shaped from the obtained picture utilizing the Secret key. A short time later, the watermark bits are removed by checking the positions of the discovery frameworks. Since the proposed watermarking strategy just uses two DCT coefficients to conceal one watermark bit, it can accomplish high installing limit. In addition, our strategy is free of host flag impedance. This coveted element and the use of a blunder cushion in watermark installing results in high power against assaults. Hypothetical examination and test comes about showing the adequacy of the proposed technique.*

Key Words: Secret Key, Computerized watermarking , Encryption and Decryption.

1. Introduction.

Networking is one of the most interesting concepts of study in the field of computer science today. Computer Networking may be seen as a branch of electrical building, media interchanges, programming designing, information development or PC outlining.

A Computer network empowers interpersonal correspondences allowing customers to pass on capably and adequately through various means: email, messaging, visit rooms, telephone, video telephone calls, and video conferencing. Offering access to information on shared stockpiling contraptions is a key part of numerous Networks. A PC Network or data Network is a media correspondences mastermind which grants center points to share resources.

Eg. The Internet!

Today facebook is one of the most popular social networking sites to share photos and text messages with our friends family members. But there are many chances of the data (photos, texts) getting hacked while we share it in facebook. Hackers are people who try to break into PC frameworks for any illicit reason or people who malevolently break into frameworks for personal gain .

1.1 Related Work.

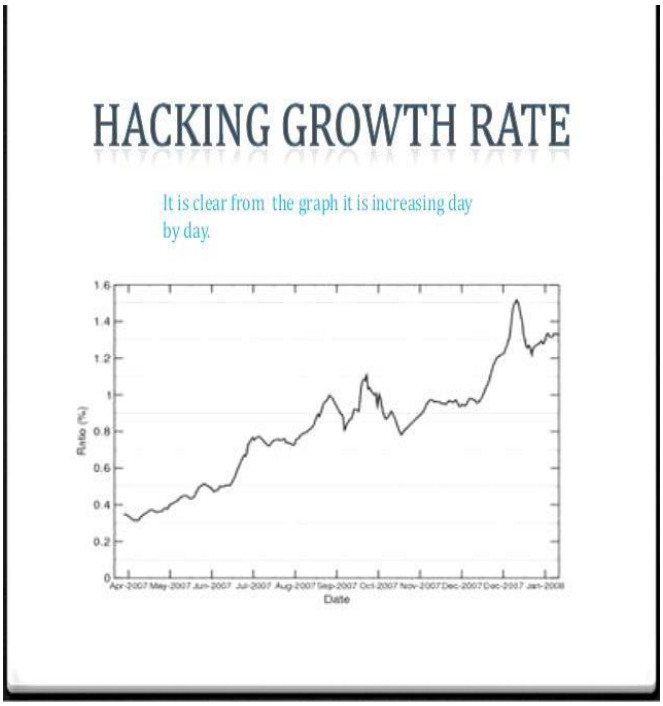
Detecting Spam on OSNs: Gao et al. [11] analyzed posts on the walls of 3.5 million Facebook users and showed that 10% of links posted on Facebook walls are spam. They also presented techniques to identify compromised accounts and spam campaigns. In other work, Gao et al. [12] and Rahman et al. [10] develop efficient techniques for online spam filtering on OSNs such as Facebook. While Gao et al. [12] rely on having the whole social graph as input, and so is usable only by the OSN provider, Rahman et al. [10] develop a third-party application for spam detection on Facebook.

In contrast to all of these efforts, rather than classifying individual posts as spam, we focus on giving protection to our account as well as the photos or text messages we send and also detect the malicious hackers who try to hack

the data that we send and notify them to the administrator.

1.2 Need for The Project.

The hacking process is done by script kiddies as well as criminal hackers.



The graph indicates that the hacking process has drastically increased over the years

The crackers hack the photos and misuse them in many ways. These hackers tread into the privacy of celebrities and individuals and also tend to manipulate the information about them and also hack the photos that they share. They publicize this tampered information and photos thereby harming the reputation of the celebrities and individuals. In order to ensure that the data that we send securely reaches the destination avoiding data breach and also from getting hacked we provide protection to our account by implementing techniques like watermarking and making use of encryption and decryption techniques adopted from PBE algorithm[Password Based Encryption] that would help the users to safely share their photos or messages among their friends selectively .It not only gives protection but also detects the Crackers who try to decrypt the images or text by entering the wrong secret key and notifies them to the administrator.

2. Existing System.

With the quick development of correspondence systems and advances in sight and sound preparing innovations, mixed media robbery has turned into a difficult issue. In an open system condition, computerized watermarking is a promising innovation to handle media information robbery. In computerized watermarking, the watermark information, (for example, distributer data, client character, document exchange/downloading records, and so on.) are covered up into the genuine sight and sound question without influencing its typical use. Whenever essential, the proprietors or law authorization organizations can separate the watermark information, by utilizing a mystery key, to follow the wellspring of illicit dissemination. While computerized watermarking can be connected to different mixed media information, for example, sound, picture and video, this paper concentrates on picture watermarking. With regards to picture watermarking, intangibility, strength, installing limit and security are of essential concerns. Up until now, different picture watermarking plans have been accounted for in the writing and a hefty portion of them were based upon systems identified with histogram minute spatial element areas spread range (SS) and quantization. In numerous applications, for example, secretive correspondence, high installing limit is craved, while heartiness against geometric assaults is not for the most part concerned. Contrasted with the watermarking techniques in, the strategies in light of SS and quantization can ordinarily accomplish higher inserting limit under given impalpability and strength.

Drawbacks Of The Existing System.

- Does not give proficiency in Secret message sharing by means of picture watermarking.
- Less security.
- The existing framework gives less adaptability.

3. Proposed system.

In this paper, we show a novel rank-based picture watermarking strategy to essentially increment implanting limit while keeping up palatable intangibility and power against normal assaults. In the proposed technique, the 2-D discrete cosine change (DCT) is connected to each picture square to acquire the relating DCT coefficients. A mystery key is used to haphazardly pick an arrangement of DCT coefficients appropriate for

inserting watermarks. The installing of watermark bits is completed by changing the arrangement of DCT coefficients utilizing a rank-based implanting principle, where a mistake cushion is additionally used to manage the blunders brought on by assaults. At the watermark identification end, we register the DCT coefficients from the got picture and afterward build the recognition frameworks utilizing a similar mystery key. The inserted watermark bits can be removed by checking the positions of the location frameworks. Contrasted and the current picture watermarking techniques, the proposed strategy has substantially higher inserting limit. In the meantime, it has high perceptual quality and is strong against normal assaults. The unrivalled execution of our technique is broke down in principle and showed by reproduction results. We use to encrypt the mystery message through Password Based Encryption calculation to secure the clients mystery messages. We add that encoded message to the watermark of every last split pictures.

Advantages of The Proposed System.

- It gives proficiency in Secret message sharing by means of picture watermarking.
- High security.
- More Flexible to share the watermark encode pictures one to many shares.

4 . Modules Description.

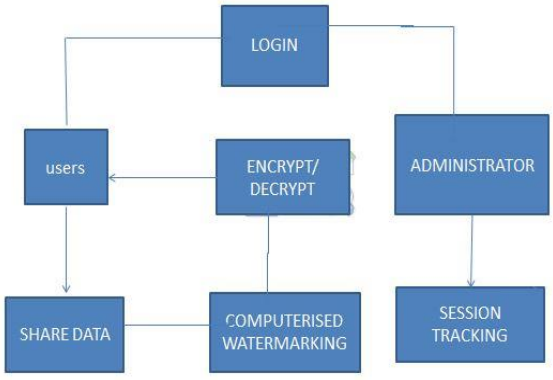


Fig 1. Architecture.

4.1 Users.

Users will register the details and log in the page, Send friend request to other users. Accept friend request. Add the images and Split the image in to four parts . Add a Secret message to the split images and convert watermark for the secret message and share in to the friends with random unique secret key via email. Received images are view by using secret random key to decrypt the secret message on out application.

4.2 Computerized watermarking

Computerized watermarking is the demonstration of concealing a message identified with an advanced flag (i.e. a picture, tune, video) inside the flag itself. It is an idea firmly identified with steganography, in that they both shroud a message inside an advanced flag. Be that as it may, what isolates them is their objective. Watermarking tries to shroud a message identified with the genuine substance of the computerized flag, while in steganography the advanced flag has no connection to the message, and it is simply utilized as a cover to conceal its reality. Watermarking has been around for a few centuries, as watermarks discovered at first in plain paper and along these lines in paper bills. Notwithstanding, the field of advanced watermarking was just created amid the most recent 15 years and it is currently being utilized for a wide range of utilizations.

Watermark- - an undetectable mark installed inside a picture to show validness or verification of ownership. It Discourages unapproved replicating and circulation of pictures over the web. It assures that an advanced picture has not been adjusted. Programming can be utilized to scan for a particular watermark. Watermark ought to seem irregular, commotion like grouping Appear Undetectable Good Correlation Properties. High connection with signs like watermark. Low connection with different watermarks or irregular commotion Common successions A) Normal dispersion B) m-groupings Watermark put into data substance of Original Image to make Watermarked Image Content Spatial Domain (Least Significant Bit) FFT - Magnitude and Phase Wavelet Transforms DCT Coefficients.

4.3 Encrypt /Decrypt.

Password based encryption (PBE) was intended to take care of issues of the kind portrayed previously. A PBE calculation creates a mystery key in light of a secret key, which will be given by the end client. As of now there are two benchmarks (PKCS #5 and #12) that characterize how a watchword can be utilized to produce a symmetric key. A decent PBE calculation will likewise blend in an irregular number called the salt alongside the watchword to make the key. Without a salt, the programmer can play out an animal drive look for the key-space no sweat. PBE is

normally utilized as a part of frameworks, for example, nearby document encryption devices, which are utilized to guarantee information secrecy. They are additionally utilized as a system to secure the client's private key store, (for example, the PKCS #8 based assurance of private keys). Client provoked passwords are normally either a subset of ASCII or UTF-8 for purposes on between operability. It ought to be noticed that UTF-8 is a super arrangement of ASCII.

The salt is an esteem that can foil word reference assaults or pre-calculation assaults. An assailant can without much of a stretch pre-figure the condensations of thousands of conceivable passwords and make a "word reference" of likely keys. Review the way that when you play out the process, changing info information even a little changes the subsequent process. By processing the secret word with a salt, the aggressor's lexicon is rendered pointless. The aggressor should look through passwords for each estimation of the salt. On the other hand, the aggressor needs to hold up until a watchword operation is performed and the salt utilized as a part of that specific operation is caught. Since the salt is arbitrary in nature, it is exceptionally impossible that a similar salt will be utilized for the following encryption handle therefore restricting the assailant assist. The salt should be created utilizing a pseudo irregular number generator (PRNG). It is additionally firmly prescribed not to reuse a similar salt an incentive for various occasions of encryption. Take note of that the salt is not a mystery esteem. In this way, it can be transmitted alongside the figure content to the collector or by means of out-of-band transmission strategies. In a perfect world the length of the salt ought to be same as the yield of the hash capacity being utilized.

4.4 Administrator.

Admin will maintain the all user details and the image attacker details on our application.

Admin maintains proper user details and track the attackers via session tracking.

4.5 Session Tracking.

All the users are tracked by session tracking. Suppose users enter the miss matched key on received images page that user will mark as an attacker on our application and sends all the proper details regarding the attacker to the administrator on our application.

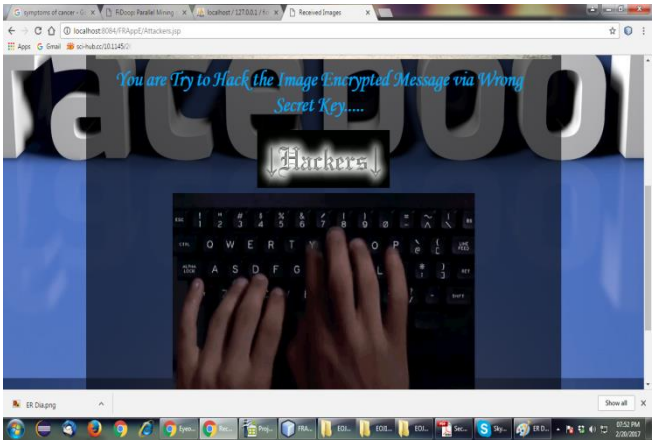


Fig 2. Depicts hackers trying to hack the data by entering the wrong secret key.

Conclusion.

The proposed technique not only detects the hackers who try to illegally hack the data that is being sent but also prevents the hackers from hacking the data by giving strong protection to the data so that they reach the correct destination .

We trust that facebook will profit by our proposals to prevent the hazard of crackers.

In future, it is possible to process all the watermarks in to videos and add the watermarks in each and every frame to enhance the security to encrypt the secret message and send to the end users globally.

REFERENCES

[1] C. Pring, “100 social media statistics for 2012,” 2012 [Online]. Available: http://thesocialskinny.com/100-social-media-statistics-for-2012/

[2] Facebook, Palo Alto, CA, USA, “Facebook Opengraph API,” [Online]. Available: http://developers.facebook.com/docs/reference/api/

[3] “Wiki: Facebook platform,” 2014 [Online]. Available: http://en. wikipedia.org/wiki/Facebook_Platform

[4] “Pr0file stalker: Rogue Facebook application,” 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report- _fb_survey_scam_pr0file_viewer_2012_4_4

[5] "Which cartoon character are you—Facebook survey scam," 2012 [Online]. Available: https://apps.facebook.com/ mypagekeeper/?status=scam_report_fb_survey_scam_whiich_ cartoon_character_are_you_2012_03_30

[6] G. Cluley, "The Pink Facebook rogue application and survey scam," 2012 [Online]. Available: http://nakedsecurity.sophos.com/2012/02/ 27/pink-facebook-survey-scam/

[7] D. Goldman, "Facebook tops 900 million users," 2012 [Online]. Available: http://money.cnn.com/2012/04/23/technology/facebookq1/index.htm

[8] R. Naraine, "Hackers selling $25 toolkit to create malicious Facebook apps," 2011 [Online]. Available: http://zd.net/g28HxI

[9] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online]. Available: http://bit.ly/b6gWn5 [10] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "Efficient and scalable socware detection in online social networks," in Proc. USENIX Security, 2012, p. 32.

[11] H. Gao et al., "Detecting and characterizing social spam campaigns," in Proc. IMC, 2010, pp. 35–47.

[12] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in Proc. NDSS, 2012.

[13] P. Chia, Y. Yamamoto, and N. Asokan, "Is this app safe? A large scale study on application permissions and risk signals," in Proc. WWW, 2012, pp. 311–320.

[14] "WhatApp? (beta)—A Stanford Center for Internet and Society Website with support from the Rose Foundation," [Online]. Available: https://whatapp.org/facebook/