ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.3

Privacy Protection against Fake Images in Social Media Using Watermarking Technique

Naveen. M[1], Thejeswaran.V[2], Sudha Rajesh[3]
Department of Computer Science and Engineering
Jeppiaar SRR Engineering College, Chennai, India

Abstract:
The a large number of dynamic clients all around the globe are utilizing on the web informal community, for example, Facebook, Twitter, Tumblr and LinkedIn. The greater parts of interpersonal organizations have powerless client to-client confirmation strategy, which depends on some essential data like showed name, photograph. These shortcomings make it to abuse the client's data and to make counterfeit profile. At the point when clients transfer the profile picture or photographs it would be watermarked and refreshed, which causes the client to remain secured against the phony profile assaults.

Keyword: Image watermarking, Integrity authentication, Image forgery detection

1. INTRODUCTION

With the quick advancement of a data arranged society, progressively huge amounts of digitalized material are being transmitted over the Internet. Concerns relating to the upgrade of security and insurance against infringement of advanced pictures have turned out to be basic over the previous decade. Computerized watermarking is currently a moderately engaged procedure went for giving a solid method to validate pictures or ensure copyrights insurance; in this system a watermark generally is installed imperceptibly in the advanced picture to abstain from pulling in the consideration of noxious assailants. As per the ideal heartiness of the implanted watermark, advanced watermarking systems are isolated into strong watermarking and delicate watermarking. The fundamental motivation behind strong watermarking system regularly is to the fast advancement of a data arranged society; progressively expansive amounts of digitalized material are being transmitted over the Internet. Concerns relating to the upgrade of security and assurance against infringement of advanced pictures have turned out to be basic over the previous decade. Computerized watermarking is presently a moderately engaged system went for giving a dependable method to verify pictures or secure copyrights insurance; in this procedure a watermark as a rule is installed imperceptibly in the advanced picture to abstain from pulling in the consideration of malignant assailants. As per the ideal power of the inserted watermark, computerized watermarking strategies are isolated into strong watermarking and delicate watermarking. The principle reason for powerful watermarking system regularly is to secure the responsibility for pictures, while the delicate watermarking strategy is utilized to confirm the uprightness of pictures. Strong watermarking is ordinarily utilized for copyright assurance, in this way it is intended to oppose assaults that endeavor to expel or decimate the watermark without essentially debasing the visual nature of the watermarked picture. In powerful watermarking, obvious watermarks of clients, for example, logos or copyright data, are inserted into the host pictures. Afterward, the verifiers can separate the watermarks and affirm possession through the watermarked pictures. Strength is one of the real purposes of concern, which implies the separated watermark must be sufficiently hearty for the responsibility for host picture to be confirmed even after the watermarked picture has been exposed to flag preparing assaults. In any case, for expanding the strength of a watermarked picture, past vigorous watermarking procedures frequently modify critical regions of the host picture, which can cause genuine bending of the nature of the watermarked picture.

This contortion may enable noxious assailants to distinguish which information are significant, enabling them to perform cryptanalysis and gain the secret information. In this manner, it is yet a remarkable issue in the watermarking field to build up a hearty watermarking plan that can convey extraordinary vigor while keeping up great visual nature of watermarked pictures. Then again, delicate watermarking was grown especially for picture verification, in which the inserted watermark ought to be delicate with the goal that any alterations of the pictures will be obvious. The validness of the picture ought to be checked absolutely if the watermarked picture has been controlled in any capacity, for example, JPEG pressure, arrangement, or editing. Since the less noteworthy regions of the host picture are changed in delicate watermarking, the visual nature of a delicate watermarked picture is normally superior to that of the hearty watermarked picture. The precision of the verification is the real worry in delicate watermarking, and procedures that were created before 2000 concentrated for the most part on distinguishing whether a picture had been messed with or not. Notwithstanding, they didn't determine unmistakably where the picture had been changed. In the course of the most recent 15 years, a few picture validation plans have been created to locate the altered regions, yet capacity of doing as such is scarcely acceptable, and only one out of every odd changed pixel is destined to be recognized effectively. Besides, the majority of the delicate watermarking plans are non-visually impaired, and unique watermark data is required amid the confirmation strategy.

2. RECENT WORKS:

OH-JIN KWON, SEUNGCHEOL CHOI, BEOMYEOL LEE," A watermark-Based Scheme for Authenticating JPEG Image Integrity", IEEE ACCESS VOL.6, 2018

Single image denoising suffers from limited data collection within a noisy image. In this paper, we propose a novel image denoising scheme, which explores both internal and external correlations with the help of web images. For each noisy patch, we build internal and external data cubes by finding similar patches from the noisy and web images, respectively. We then propose reducing noise by a two-stage strategy using different filtering approaches. In the first stage, since the noisy patch may lead to inaccurate patch selection, we propose a graph based optimization method to improve patch matching accuracy in external denoising. The internal denoising is frequency truncation on internal cubes. By combining the internal and external denoising patches, we obtain a preliminary denoising result. In the second stage, we propose reducing noise by filtering of external and internal cubes, respectively, on transform domain. In this stage, the preliminary denoising result not only enhances the patch matching accuracy but also provides reliable estimates of filtering parameters. The final denoising image is obtained by fusing the external and internal filtering results. Experimental results show that our method constantly outperforms state-of-the-art denoising schemes in both subjective and objective quality measurements, e.g., it achieves >2 dB gain compared with BM3D at a wide range of noise levels.[1]

"CID: Combined image denoising in spatial and frequency domains using web images, Huanjing Yue; Xiaoyan Sun; Jingyu Yang; Feng Wu, Jun., 2014 IEEE Conference on Computer Vision and Pattern Recognition.

A novel two-step scheme to filter heavy noise from images with the assistance of retrieved Web images. There are two key technical contributions in our scheme. First, for every noisy image block, we build two three dimensional (3D) data cubes by using similar blocks in retrieved Web images and similar nonlocal blocks within the noisy image, respectively. To better use their correlations, we propose different denoising strategies. The denoising in the 3D cube built upon the retrieved images is performed as median filtering in the spatial domain, whereas the denoising in the other 3D cube is performed in the frequency domain. These two denoising results are then combined in the frequency domain to produce a denoising image. Second, to handle heavy noise, we further propose using the denoising image to improve image registration of the retrieved Web images, 3D cube building, and the estimation of filtering parameters in the frequency domain. Afterwards, the proposed denoising is performed on the noisy image again to generate the final denoising result. Our experimental results show that when the noise is high, the proposed scheme is better than BM3D by more than 2 dB in PSNR and the visual quality improvement is clear to see.[2]

DETECTING FAKE PROFILES IN ON-LINE SOCIAL NETWORKS, MARCO SECCHIERO, MAURO –CONTI, AUGUST 2012 IEEE/ ACM INTERNATIONAL CONFERENCE ON ADVANCES IN SOCIAL NETWORKS ANALYSIS AND MINING

On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Like the cyberspace in Internet, the OSNs are attracting the interest of the malicious entities that are trying to exploit the vulnerabilities and weaknesses of the OSNs. Increasing reports of the security and privacy threats in the OSNs is attracting security researchers trying to detect and mitigate threats to individual users. With many OSNs having tens or hundreds of million users collectively generating billions of personal data content that can be exploited, detecting and preventing attacks on individual user privacy is a major challenge. Most of the current research has focused on protecting the privacy of an existing online profile in a given OSN. Instead, we note that there is a risk of not having a profile in the last fancy social network! The risk is due to the fact that an adversary may create a fake profile to impersonate a real person on the OSN. The fake profile could be exploited to build online relationship with the friends of victim of identity theft, with the final target of stealing personal information of the victim, via interacting online with the friends of the victim. In this paper, we report on the investigation we did on a possible approach to mitigate this problem. In doing so, we also note that we are the first ones to analyze social network graphs from a dynamic point of view within the context of privacy threats.[3]

3. PROPOSED SYSTEM:

3.1. MODULES

1. USER ENROLLMENT
2. SECURING IMAGE
3. INTRUSION DETECTION SYSTEM
4. ALERT AND BLOCK

3.1.1.USER ENROLLMENT:

Here the client register with their subtleties to join up with any social media. User enter the client name and secret phrase and different subtleties for the future use. User then login to the specific internet based life.

3.1.2 SECURING IMAGE.

After the enlistment of the client with their details. If the client wishes to transfer the image, the picture that he chose will be watermarked with username. And gets uploaded into the server and put away in database

3.1.3INTRUSION DETECTION SYSTEM:

Framework will naturally check the privilege and benefit of the client and responsibility for document. Along these lines to checking the transferred picture, if the framework finds the presence of watermark. It will send a declaration and a warning to the proprietor of unique substance and keep User from re-transferring.

3.1.4. ALERT AND BLOCK:

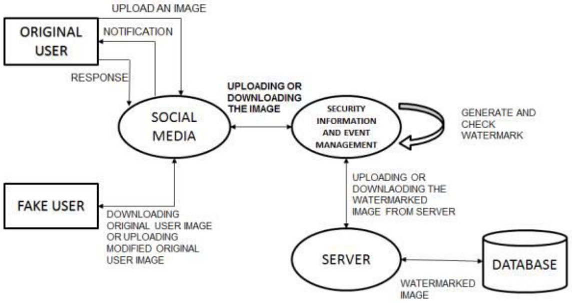
On the off chance that the framework finds the presence of watermark, it will send a notice to the proprietor of unique substance and keep Fake client from re-uploading. Fake clients refreshing a similar profile picture can be recognized and their particular macintosh address would be followed and blocked.

4. SYSTEM ARCHITECTURE:

Our system architecture includes three main entities:

- Securing the image while uploading into any social media through watermarking technique.

- Detection based on watermarking.
- Alerting the corresponding user.


UPLOAD AN IMAGE
ORIGINAL USER
NOTIFICATION
RESPONSE
SOCIAL MEDIA
UPLOADING OR DOWNLOADING THE IMAGE
SECURITY INFORMATION AND EVENT MANAGEMENT
GENERATE AND CHECK WATERMARK
FAKE USER
DOWNLOADING ORIGINAL USER IMAGE OR UPLOADING MODIFIED ORIGINAL USER IMAGE
UPLOADING OR DOWNLAODING THE WATERMARKED IMAGE FROM SERVER
SERVER
DATABASE
WATERMARKED IMAGE

The first client here is the proprietor who endeavors to have protection in online life ,the client transfers the picture in the web-based social networking where the Security Information and Event Management(SIEM) makes the watermarking on the client picture and gets spared in the database. Presently, if any client who endeavors to download or transfer the picture the SIEM checks whether the picture is as of now watermarked or not if so the first client gets the alarm message or notice that client attempting to download the picture, contingent upon the first client reaction the anther client can download the picture or transfer the picture.

5. ALGORITHM:

5.1Embedding the invisible robust watermark:

Initially, the original RGB color image is converted into YCbCr color space. The basic equations used to convert RGB into YCbCr are:

$$Y=0.299R+0.587G+0.114B$$

$$Cb=-0.172R-0.339G+0.511B+128$$

$$Cr=0.511R-0.428G-0.083B+128$$

(1)After YCbCr conversion, the one level DWT decomposition of Yis performed to generate the low-low(LL),low-high(LH), high-low (HL), and high-high (HH) sub-bands, where LL consists of the approximation part of the original Y channel, and the remaining three resolution sub-bands consist of the detailed parts, which are very difficult for the human eye to discern. Thus, we used this characteristic for our robust watermarking scheme.

Table .5.Luminance quantization table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

First the LL sub-band is divided into several 8⌟8-sized blocks, and, then, each pixel sofa block is quantized by directly dividing it by the corresponding value of the luminance quantization table which is defined by U. It [11], as shown in Fig. 2. After all of the blocks have been quantized, a quantized LL (Q-LL) sub-band is generated, and the HH sub-band is replaced directly by the resulting Q-LL sub-band. This is because the quantized LL sub-band would hardly be changed while suffering malicious attacks. This characteristic allows the blind and robust decoding during watermark extraction procedure. After that, the robust watermark is embedded in the Q-LL sub-band to produce a watermarked quantized LL (WQ-LL) sub-band with the following equation:

$$WQLL_n=QLL_n+W_{Rn}*k,$$

Where QLL_n is the pixel value in the Q-LLsub-band, $WQLL_n$is the resulting pixel value in the WQ-LL sub-band, WR_n is the embedded robust watermark bit, and k is a constant parameter that corresponds to the strength of the watermark. A higher k can increase the strength of the embedded watermark, but it makes the watermarked image easier to perceive. After embedding the watermark, the inverse DWTs of the four resulting sub-bands, i.e., LL, HL, LH, and WQ-LL, are performed to generate the watermarked Y' channel. Then, the watermarked Y', Cb, and Cr channels are converted back into RGB and saved as the robust watermarked image.

6. CONCLUSION:

This paper introduces a short learning about the assaults and resistance instruments, which are unmistakable on Online Social systems. It likewise clarifies the work, which had been performed in the field of distinguishing counterfeit profiles. In this venture, discrete wavelet change calculation is proposed for data stowing endlessly. Thusly this would keep the phony ambushes and giving total customer data security ensuring.

7. REFERENCE:

[1]. OH-JIN KWON, SEUNGCHEOL CHOI, BEOMYEOL LEE, " A watermark-Based Scheme for Authenticating JPEG Image Integrity", IEEE ACCESS VOL.6,2018

[2].A.Khan, S.A.Malik, "A high capacity reversible water marking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection," Information Sciences, vol. 256, pp. 162-183,2014.

[3]. W. J. Chen, C. C. Chang, T. H. Ngan Le, "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, pp.3292-3301,2010.

[4].5Q. Su, Y. Niu, H. Zou, X. X. Liu, "A blind dual color images watermarking based on singular value decomposition," Applied MathematicsandComputation,vol.219,no.16,pp.8455-8466,2013.

[5].S. P. Maity, S. Maity, J. Sil, C. Delpha, "Collusion resilient spread spectrum watermarking in M-band wavelets using GA-fuzzy hybridization," Journal of Systems and Software, vol. 86, no.1, pp.47-59, 2013.

[6]. C. S. Lu, H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1579-1592,2001.

[7].P.Y.Lin,J.S.Lee,C.C.Chang,"Dualdigitalwatermarkingforinternet media based on hybrid strategies," IEEE Transactions on

Circuits and Systems for Video Technology, vol. 19, no. 8, pp. 1169-1177, 2009.

[8].F.Lusson, K.Bailey, M.Leeney, K.Curran, “Anovel approach to digital watermarking, exploiting colour spaces,” Signal Processing, vol. 93, no. 5, pp. 1268-1294, 2013.

[9]. C.C.Lin, Y.H. Chen,C.C. Chang, “LSB-based high-capacity data embedding scheme for digital images,” International Journal of Innovative Computing, Information and Control, vol. 5, no. 11, pp. 4283-4289,2009.

[10].Int. Telecommunication Union, “Information technology-digital compression and coding of continuous -tonestillimages-requirements and guide lines,” CCITT Recommendation T.8 1, 1992.

[11]. L. Zhang, L. Zhang, X. Q. Mou, D Zhang, "FSIM: A feature similarity index for image quality assessment", IEEE Transactions on Image Processing, vol. 20, no. 8, pp. 2378-2386,2011.

[12]. R. Z. Wang, C. F. Lin, J. C. Lin, "Image hiding by optimal LSB substitution and genetical gorithm," Pattern recognition, vol. 34,no.3,pp. 671-683,2001.

[13].Q. Su, Y. Niu, X. Liu, Y. Zhu, “A blind dual color images watermarking based on IWT and state coding,” Optics Communications, vol.285,no.7, pp. 1717-1724,2012.