IMAGE SECLUSION TRESPASSING IN OSN USING WATERMARKING TECHNIQUES

[1]Murugeasan M
Assistant Professor
Computer Science and Engineering,
M. Kumarasamy College of Engineering, Karur,
Tamil Nadu, India.
murugankathir@gmail.com

[2]Britto Edison R
Computer Science and Engineering,
M. Kumarasamy College of Engineering, Karur,
Tamil Nadu, India
brittosharoncserf@gmail.com

[3]Joy Maria Ancy J
Computer Science and Engineering,
M. Kumarasamy College of Engineering, Karur,
Tamil Nadu, India
aancyboscoj@gmail.com

[4]Jegan Kumar T
Computer Science and Engineering,
M. Kumarasamy College of Engineering, Karur,
Tamil Nadu, India.
Jkjegankumar96@gmail.com

***Abstract*—**A social networking service (additionally social networking website online, SNS or social media) is an online platform that is utilized by humans to construct social networks or social relations with different individuals who proportion similar non-public or career pursuits, activities, backgrounds or real-existence connections. Social networking sites are various and that they comprise a selection of latest information and communique tools which include availability on computer and laptops, cell gadgets inclusive of tablet computers and smart phones, digital photograph/video/sharing and "web logging" diary entries on-line (blogging). While Online Social Networks (OSNs) permit users to share snap shots without difficulty, they also divulge customers to numerous confinementthreats from each the OSNs and external entities. Image over the social network is transferred or transmitted among servers and a couple of customers. Privacy of that statistics could be very important as it belongs to personal touchy facts. In present gadget, textual content primarily based encryption can be implemented in social networks. There are many extraordinary approached of storing data securely over the social networks, using large records together with give up-to-stop encrypted facts transmission, dynamic credential era best for textual content data. In this paper, can introduce a novel watermarking scheme with wavelet set of rules named as discrete wavelet rework in actual time social community utility. In this scheme can use images and saved in server in cozy format. And also make bigger the paper, categorize the image as sensitive or normal. If it's miles touchy manner, perform copyrights algorithms. Then offer the permission to the receiver end for download the images in comfortable manner. And also implement safety controls to dam mouse operations and print display options. Experimental result may be suggests that during real time social community environments and comparative observe of existing algorithms based on computational time and confinement rate.

Index Terms—**Online social networks, Image Acquisition, Privacy violations, Digital watermarking techniques, Wavelet co-efficient values**

I. INTRODUCTION

In today's years, online Social Networks (OSNs) have attracted many hundreds of thousands of customers worldwide. Even though Social Networks have perpetually been a primary part of day-to-day life, now that more and more oldsters are connected to the internet, their on-line counterparts are enjoyable a more and more essential feature. OSNs have also grown to be a scorching difficulty in regions of research ranging from sociology to computer technological know-how and arithmetic. Except for enabling customers to create a community to symbolize their social ties, many OSNs facilitate importing of multimedia content material cloth, pretty quite a few techniques of communiqué and sharing many factors of everyday lifestyles with friends. Humans can keep in contact with (bodily some distance off) acquaintances, pretty certainly percentage content cloth and experiences and hold up-to-the-minute within the alleviation in their own domestic or whilst at the flow. Social network systems offer an easy human computing device interface for internet clients, making it clean to proportion unlimited-shape statistics (equal to photographs and films) with buddies wherever and whenever. Additionally, clients can revel in real-time and unfastened chats with others, post the brand new status updates/affirm-ins, and categorical critiques about present social sizzling spots. On the grounds that social networking's introduction, we've substantive a few massively advantageous structures emerge (including fb, Twitter, and Instagram). When surfing on such systems, most clients are blind to the platform's privacy troubles; however truly, users' social community privacy is primary. Some touchy information equal to a personal alternative, profile, and shared photos will be leaked to others who aren't granted entry rights, if the social media carrier supplier doesn't take first-class precautions to protect entry manipulate. It's plain that most of the people social community platforms intention to preserve their consumers' privacy as loads as they may be capable of. Nevertheless, blessings aside, advantage threats to user privacy are extra frequently than no longer underestimated. For example, due to the general public nature of many OSNs and the internet itself, content material can easily be disclosed to plenty broader viewers than the individual intended. Users extra frequently than no longer have drawback revoking or

deleting understanding and information some customers would possibly also be posted by way of using others without their consent. Confinement in OSNs is a complicated remember and isn't at all times intuitive to clients, specially whilst you take into account that it's on no account instances similar to how privacy works in real-existence interactions. Ideally, clients need to be successful to alternate a few confinements for functionality, without their know-how becoming handy past the scope they intend. For instance, a customer of self-help OSN would like to satisfy parents with the same medical scenario however does not want every person to recognize about his ailment. Even in a great deal much less extreme times, the price of confinement is most of the time underestimated. In this paintings, we spotlight that the essence of the scenario is that present mechanisms for outlining entry to pics in OSNs, cannot honestly control instances in which the involved parties have conflicting settings. First, the photo uploaded is regarded the owner of the snapshot and is granted full rights, whereas the oldsters displaying in the photo must no longer seemed co-homeowners and have to no longer granted any rights. On high of this well-known coarse-grained procedure, OSN companies put into effect additional insurance policies, a number of so that it will significantly complicate problems. Moreover, any users which can be tagged have an effect at the visibility of the image, because the picture will likely be viewable by way of all their contacts (default privacy environment). Therefore, even when the users tagged within the photo have confined its visibility, if the uploaded has now not confined entry the photograph will in all likelihood be publicly available, something which the remainder users isn't always going to even be conscious of. Generally, these events may also be characterized as cases of conflicts of hobby, the location they want of the content material cloth author goes in the direction of the choice of the depicted users, or the privacy settings of consumer override those of 1 other. Note that although the access manipulate mechanisms may want to range at some stage in OSNs, conflicts of hobby are a normal impediment, as they stand up from the content material fabric of the snap shots. The various varieties of social networks are proven in figure 1.

Fig 1: Social Networks

.

II. Related Work

H. Cheng, X. Zhang, et.al, [1] Proposed a unique scheme for encrypted JPEG graphics, where intra-block, inter-block, and inter-aspect dependencies among DCT coefficients are introduced. With this scheme, the encrypted JPEG snap shots also can be sold via a combination of the glide cipher and permutation encryption and outsourced to a server. And further, with the given encrypted question picture and the encrypted database snap shots, it's miles convenient for the server to calculate their similarities in encrypted domain via using the processes of a Markov method and multi-category guide vector pc (SVM). As the cause of the scheme is to deal with the challenge of image retrieval in encrypted domain even as keeping the record length and structure compliance for JPEG photos, proper right here, we first take a partial picture encryption approach beneath consideration to encrypt JPEG photos. The predicament is elaborate to clear up for the common cryptography. Probably the most current partial encryption structures for JPEG images are often situated on blocks shuffle, DCT coefficient permutation, and encrypting the signs of DCT coefficients. The proposed encryption method aren't able to simplest meet the necessities of layout compliance and document length upkeep but in addition grant priceless information regarding the period of each variable length integer (VLI) code for DCT coefficients. It means that it is easy to nonetheless accumulate the authentic size of any VLI code concerning DCT coefficients from an encrypted JPEG image. Because of the dependencies of DCT coefficients in everything, their corresponding VLI code size should have same relationships, which may also be exploited to generate characteristic for photograph retrieval.

A. Rial, M. Deng,et.al,… [2] Combining encryption with virtual watermarking, a purchaser–seller watermarking (BSW) protocol is correctly an uneven fingerprinting protocol the location the fingerprint is embedded by way of the use of watermarking in the encrypted region. The elemental inspiration is that every consumer obtains a barely specific replica of the digital content material provided by using the vendor. This sort of exchange, the watermark (or fingerprint), does now not harm the perceptual best of the digital content and can't be effortlessly removed thru the buyer. Due to the latter assets, when a malicious consumer redistributes a pirated reproduction, the seller can associate the pirated reproduction to its buyer through its embedded watermark. On the alternative hand, a malicious dealer aren't able to frame an honest consumer due to the truth the client's watermark and the brought watermarked content material are unknown to the seller. The main contribution of labor is a formal protection evaluation of BSW protocols. And hire the high-quality-world/actual-global paradigm to define security of nameless BSW protocols. With appreciate to classical choppy fingerprinting schemes, which outline every safety property one at a time, this definition outcomes inside the development of protocols that are secure below composition. The definition is common in the texture that it captures the safety homes required for any copyright protection protocol that offers customers with anonymity. Moreover, we outline protection for blind and readable watermarking schemes, and analyze the homes that watermarking schemes need to provide for the development of relaxed BSW protocols.

J. Zhang, Y. Xiang,et.al,..[3] Implemented content-based photo retrieval (CBIR) is a charming software that can be achieved more effectively on cloud computing. CBIR goals to go looking virtual pics from full-size photo records gadgets installed on their visible content material described with the useful resource of factors along with shade, texture and form. On cloud computing, CBIR systems can serve extra effortlessly by means of saving the computation time of photograph evaluation and buying. The immoderate efficiency and adaptability of cloud computing may additionally improvement the deployment of CBIR structures. First, the contributors and their roles in a picture retrieval watermarking protocol are superb from the ones in a purchaser–dealer watermarking protocol. In a customer–supplier watermarking protocol, the seller is the owner of a virtual content material cloth, who conducts the watermark insertion, and the customer can receive a watermarked digital content material fabric. In evaluation, in an picture-retrieval watermarking protocol, the consumer is the proprietor of a question image, who ought to insert a watermark to safeguard its proper, and the issuer provider of CBIR will search photos in line with the watermarked question picture acquired from the customer. The alternate makes some present safety options inapplicable; e.g. the answer of the unbinding issue for a customer–seller watermarking protocol is inapplicable in a photo-retrieval watermarking protocol.

T. Bianchi and A. Piva, et.al,… [4] Has been addressed introducing at ease watermark embedding, it's mechanisms the vicinity the watermark embedding is carried out in a way that the content cloth owner does now not have get entry to the final watermarked variation, even as no longer disclosing the commonplace content material cloth. Options exist to safely and correctly embed a watermark each at the server's side and at the client's aspect. Relaxed server-side embedding may be applied as a building block in asymmetric fingerprint protocols, supplying a cryptographically cozy method to the purchaser's rights impediment, at the equal time secure consumer-factor embedding provides an awfully efficient option to the method scalability venture. The presence of entrusted verifiers can also be solved by resorting to at ease watermark detection, i.e., to an interactive evidence scheme the location the content material proprietor convinces a further fascinated get together that his/her content fabric carries a given watermark without disclosing touchy information that could facilitate the watermark removal, just like the key of the watermarking algorithm or the actual watermark. In the subsequent sections, we can illustrate the aforementioned tactics, looking for to furnish the reader with a obvious running out in their merits and their praise barriers. The paper will quit with a dialogue about possible new studies commands, specializing in take a look at challenges which can be specifically fascinating for the sign processing neighborhood.

A. Piva, T. Bianchi,et.al,… [5] Represented through the consumer-aspect watermark embedding: on this case, a server–patron structure is yet again adopted; although, in this example, the server is permitted to deliver a detailed duplicate of the content material to all the clients with the aid of broadcasting techniques, without the have to generate one-of-a-type watermarked copies (hence removing the bottlenecks reward in the server-factor watermark embedding process); instead, each purchaser shall be in control of embedding a individual watermark determining the acquired duplicate. On this case, however, considering that the clients are entrusted, appropriate alternatives need to be devised no longer to allow malevolent customers to have got right of entry to the common content material fabric or to the watermark to be inserted. A new approach, mentioned as comfortable watermark embedding, has been proposed for going thru this kind of problem: here, the server transmits the identical encrypted version of the long-set up work to all of the purchasers, however a customer-distinctive mystery makes it possible for decryption of the content material and at the identical time implicit embedding of a customized watermark, acquiring a uniquely watermarked version of the work. In distinct, we safely designed an LUT-established at ease consumer-side embedding method enabling us to embed a spread end up dither modulation (ST-DM) watermark. As it's far going to be verified inside the following sections, this alteration shouldn't be easy; while you recall that the consumer-aspect embedding framework imposes a few constraints that do not allow us to embed a natural ST-DM watermark. Nonetheless, the experimental effects will verify that the prevalence of ST-DM versus SS watermarking exhibited inside the classical embedding schemes is maintained additionally within the purchaser-aspect embedding manner.

III. EXISTING WORK

Social networking web sites might be a new international to create social family individuals amongst human beings that proportion facts like text, picture, videos, activities, pursuits, backgrounds or day-to-day-life connections. A social community issuer consists of an instance of every user (commonly a profile), his or her social links, and number further offerings. Social network internet web sites are an internet-primarily based provider that lets in humans to make a public profile, to make a list of users with whom to proportion connections, and evaluate and move the connections in the method. Probably the most nicely-preferred social networking websites are face-eBook, Gmail, yahoo, LinkedIn, Google plus, Twitter, and plenty of others. Communications over the Social Networks don't appear to be secure. Many attacks and violation of privacy are lately confronted in our most elegant networking web sites. We use the social networking web sites for speaking to our buddies and sharing digital know-how like textual content, snap shots, video and so forth. After we percentage a digital statistics to our friends; the know-how may just face a few attacks from the attackers and/or unauthorized customers. In the direction of this verbal exchange replacement legal users or third parties shouldn't be involved. Any unauthorized customers make a try to attack a communication that is attempting to get entry to the picture for modifying or misusing. The attacker's best reason is to make crime utilizing the personal digital facts from social networking websites. The attacker tries to assault the conversation in masses of approaches i.e., violates the privacy, records attacking from the servers, etc.

3.1 RDH established method:

The present process is to guard extraordinarily non-public, different or secret understanding from unauthorized customers. Here, privacy safety is a maximum essential limitation of many social networking websites. And

paintings utilizing Reversible statistics Hiding (RDH) techniques go to gather its significance as a consequence of the exponential growth and mystery verbal exchange of capabilities man or woman over the net. All social networking web sites' architectures include range of servers, databases, web site, records like text, image, and video and so on. In existing paintings, consumer try to upload an image, the frontend program embed some confinement facts into the photograph using Reversible statistics Hiding (RDH) gadget utilizing and additionally retailer encrypted snapshot into database. To showcase this photograph on friend's wall, the frontend software exams the pix embed privacy knowledge suit with buddy's confinement knowledge. If each confinement information's are equal, then best the snapshot is visible to the acquaintances. Or else, the person is not a pal so the photo simply is not apparent. Right here, first gadget is embedding and second one is to maintain the encrypted image into database. Ordinarily of know-how hiding, the picture will expertise a few distortions because of understanding hiding and cannot invert again to the original photograph item. That's, some parameter distortion has befell to the duvet object even after the hidden records were extracted out. Within the Reversible expertise hiding, each photo and information are equally principal. The Reversible records hiding gadget, the customary cover item lossless recovered after the message is extracted.

The prevailing framework is shown in fig 2.

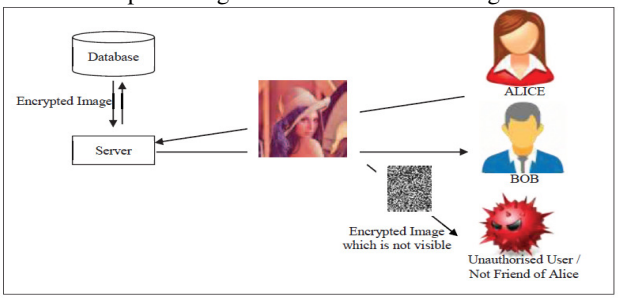

Fig 2. RDH framework

3.2 Broadcast encryption scheme:

The improvement of confinement-keeping information is accomplished with the aid of the data owner on every occasion man or woman records want be shared. The essential concept is that the info owner has proper manage over get right of entry to his/her non-public records, notably the ones revealing identification knowledge and personal lifestyles (e.g., photographs, motion pictures, copyrighted materials). More typically, the facts proprietor could act as a group manager who classifies contacts consistent with their roles (e.g., family, coworkers, and excessive college classmates, wearing activities membership members) and materials them the corresponding memberships. Every function defines a subgroup, the individuals of which can be restrained to targeted understanding classes. A knowledge category is created by using the information owner describing the set of statistics files that can be accessed as an entire with the aid of way of 1 or more subgroups. The granularity of information instructions is adjustable depending at the fineness of preferred access manage. For example, while the types are coarsely mentioned as track, films, pix, my testimonies, and so on, a subgroup of contributors who're permitted to a class can entry the complete information in that class. This is typically undesirable because the data proprietor can also want to free up awesome information only to related men and women (e.g., loved ones pix or videos handiest to be had to cherish ones people). The records owners could have the liberty to create their own lessons situated on the quantity and type of their subgroups, which is a design dilemma and will not be elaborated extra. Broadcast encryption permits for a applicable transmitter to send encrypted knowledge to a set of customers such that high-quality a privileged subset of users can decrypt the facts. Broadcast encryption is designed for and in large part implemented in the at ease distribution of copyrighted media over the net. The posted encryption steps will also be defined in fig 3. Other features of broadcast encryption contain encrypted document structures (e.g., home windows EFS) for constrained record sharing, mailing file programs for sending exceptional emails, and so forth. This requirement states that facts privacy is preserved within the presence of collusion attacks the location two or greater entities collude to obtain extra data at the sufferer than what is available to each colluding man or woman.

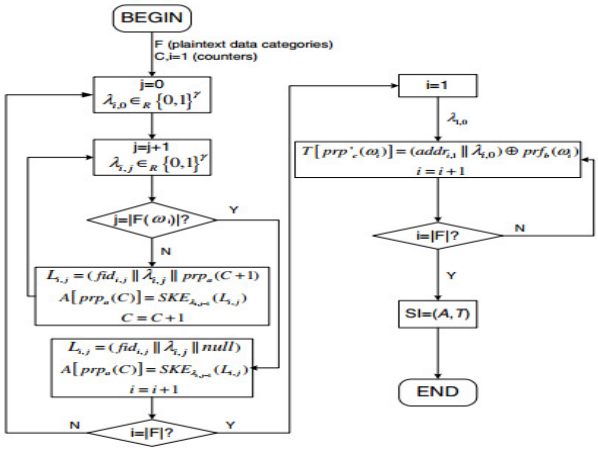

Fig 3: Broadcast encryption

IV. PROPOSED FRAMEWORK

Images at the social networks, execute 3 main protection traits: Confidentiality, Integrity and Authenticity. Confidentiality means that simplest the entitled humans have the access to the particular images, as a result tagging.

Integrity way the picture has not been modified through non-accredited man or woman.

Authenticity is the evidence that picture has indeed the extraordinary individuals as proven, or is a modified variation using the quite a number photograph processing programs.

The increment within the development and use of software image editors has accompanied the increase in the tampering of these normal traits. Specifically, the flourishing use of social networks has made the sharing and distribution of photos quite handy. The integrity and authenticity is the compelling question as, amongst exclusive fields, those pictures are also being used as proof in the courts of law. It is extraordinarily crucial to verify the integrity of these photos and is most often captivating to establish if a photo has been manipulated from the time of recording. To have knowledge of, how things cross inside

the history of a jpeg photograph, we can put into effect watermarking process to cover default pattern into image. Watermarking also can be accomplished making use of discrete wavelet turn out to be. In numerical evaluation and beneficial analysis, a discrete wavelet change into (DWT) is any wavelet remodel for which the wavelets are discretely sampled. As with exceptional wavelet transforms, a key capabilities it has over Fourier transforms is temporal resolution: it captures every frequency and region understanding (vicinity in time). Water mark bits are embedded into photo. The discrete wavelet grows to be algorithm is outlined in fig 4.

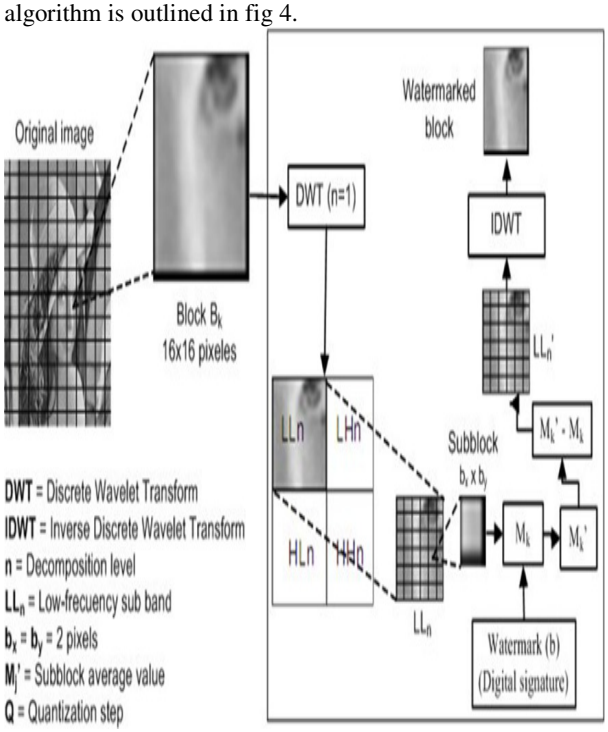

Fig 4: Discrete wavelet steps

Based in inverse DWT, we will get the scene water mark that can be restored into customary image. In the interface aspect, we will exchange the color of textual content pixels into color of photograph pixels. So photo may also be considered as undeniable content. Headquartered on this atmosphere, hacker complicated to grasp in regards to the photograph safety. Person can set confinement settings to dam the pictures to down load by way of third parties. So unauthorized users most effective get watermark information handiest. Then utilizing disable options in mouse right click on and print reveal options. Snapshot confinementis maintained in social networks. Furthermore, the concept of blacklists and their administration are not believed by any of these access control models. The application of content-based filtering on messages posted on OSN user walls poses additional challenges given the short length of these messages other than the wide range of topics that can be discussed. Short text categorization has acknowledged up to now few attentions in the scientific community. This classifier will be used in hierarchical strategy. The first level task will be classified with positive and negative labels. The second level act as a negative, it will develop gradual membership. This grade will be used as succeeding phases for filtering process. Short text classifier includes text representation, machine learning based classification. The proposed framework is shown in fig 5.

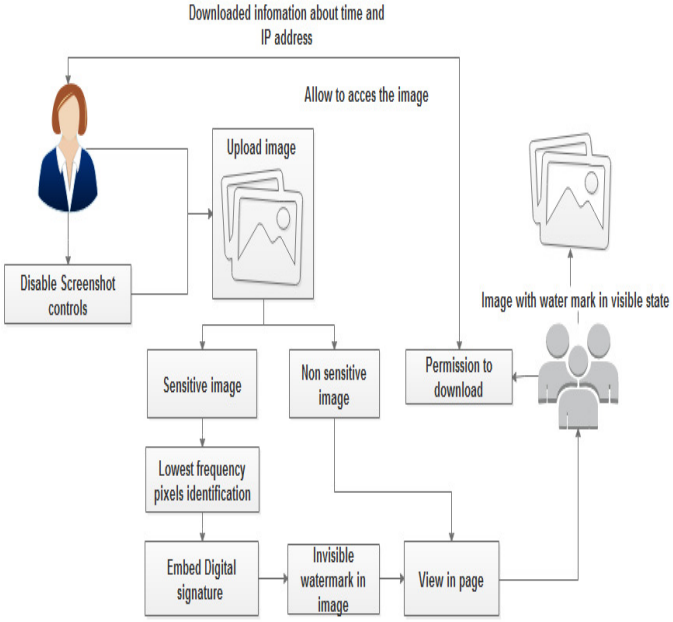

Fig 5: Proposed Framework

V. METHODOLOGIES

SNS have emerged as very famous considering that they have many attracting capabilities for the customers. Most social networking web sites allow member to design their own profiles so as to design their profile web page so that it will specific themselves and to mirror their character. Users can customize the profile layout, add applications and may upload pix and different kind of information. SNS also carries Friends listing, containing different customers of SNS. Through SNSs users can preserve in contact with friends and circle of relatives, they could locate antique pals; contact buddies of friends, and even can touch humans they didn't previously known at all. Some SNSs also assist customers to find a activity or set up enterprise contacts, together with connecting with customers, partners and in locating out jobs and commercial enterprise possibilities

5.1 Social network creation:

Social community refers to interplay among human beings wherein they create, percentage, and/or change information and ideas in virtual groups and networks. A social community supervisor is the character in an organization depended on with monitoring, contributing to, and filtering, measuring and otherwise guiding the social media presence of a logo, product, individual or corporation. In face e book, GUIis a sort of person interface that allows customers to engage with customers through graphical icons and visible indicators inclusive of secondary notation, instead of textual content-based interfaces, typed command labels or textual content navigation. In this module, we are able to have 3 kinds of users consisting of image owner, picture users and image server. Image proprietor may be adding the photo into system and photograph server shops the pictures in database. Image customers use pics which might be shared by photo owner.

5.2 Upload image:

The first level of any sharing gadget is the photo acquisition level. After the image has been obtained, diverse techniques of processing can be carried out to the image to carry out the various exceptional imaginative and prescient obligations required these days. However, if the image has now not been acquired satisfactorily then the meant tasks might not be practicable, despite the useful resource of a few form of photo enhancement. The basic -dimensional photo is a monochrome (greyscale) picture which has been digitized. Describe picture as a -dimensional light intensity characteristic f(x,y) wherein x and y are spatial coordinates and the cost of f at any point (x, y) is proportional to the brightness or gray cost of the picture at that point. In this module, we will upload various photographs which include herbal pics, face pictures and other pix. Uploaded pics can by way of any type and any size.

5.3 Embed the watermark:

In this module, we can embed the watermark text into pictures. Digital media can be saved correctly and can be manipulated very without difficulty the use of computers, resulting in numerous safety troubles. The hassle of defensive the copyright of digital media may be solved by virtual watermark. Digital watermarking is an idea of hiding possession statistics into the multimedia facts, which can be extracted in a while to prove the authenticated proprietor of the media. Watermarking guarantees authenticating possession, protecting hidden records, prevents unauthorized copying and distribution of pics over the internet and guarantees that a virtual picture has now not been altered. We can implement Discrete Wavelet Transform (DWT) area image watermarking system for real time photograph. In the embedding method, the watermark may be encoded into the cover photograph using a particular area. This location values is used to shield the photos. The output of the embedding technique, the watermarked picture, is then transmitted to the OSN home web page.

5.4 Privacy settings:

Each user photos are first labeled into confinement coverage. Then confinement rules of every pix may be categorized and analyzed for predict the coverage. So we adopting levels approach for policy recommendation than applying the common one-degree facts mining tactics to mine both image capabilities and regulations together. The two-stage approach permits the system to appoint the primary stage to classify the policy as with privacy or without privacy. In the second level, we can set without privacy manner, pick the person list information.

5.5 Protection system:

In this module, we are able to set the safety or blocking gadget to avoid 1/3 celebration aces without knowledge of photograph owners. This module is used to set the photograph with privacy. If consumer set with confinement settings approach, all users are taken into consideration as 0.33 events. Based in these putting, unauthorized consumer most effective perspectives the photo and can't be used. If he downloads approach, best get water mark values. Finally provide hardware control system consisting of mouse controls and keyboard controls. Then disable the mouse operations and gadget print display screen alternatives. Mouse code and print display controls values are extracted and to provide coding implementation to disable the coding as fake settings. We can enforce this idea in all browsers and to put into effect in all pics which are shared via social users.

VI. CONCLUSION

The appearance of famous on line social networking has precipitated in the compromise of conventional notions of privacy, really in visible media. With a view to facilitate useful and principled protection of picture privacy online, we've were given furnished the layout, implementation, and evaluation of picture protect machine that correctly and effectively protects purchaser's image privacy throughout well-known OSNs. The virtual watermarking method primarily based fully on DWT coefficients amendment for social networking services has been presented on this paper. In the embedding manner, the coefficients in LL sub-band had been used to embed watermark. Within the extraction process, everyday coefficient prediction primarily based on mean clear out is used to boom the accuracy of the extracted watermark. On extending the Machine Learning (ML) textual content categorization techniques to automatically assign with each quick textual content message a fixed of classes based on its content material. Then exploiting a bendy language to specify Filtering Rules (FRs), through which customers can kingdom what contents, should now not be displayed on their partitions. FRs can assist a ramification of various filtering criteria that can be combined and customized in keeping with the person desires. As part of destiny paintings, to implement cryptographic techniques and various were filtering strategies to comfy OSN domestic web page. And also enlarge the paintings in confinement primarily based uploaded video content sharing web sites. The experimental final results showed a bigger universal performance in unique time software.

REFERENCES

[1] H. Cheng, X. Zhang, J. Yu, and F. Li, "Markov process based retrieval for encrypted jpeg images," in Proc. of 10th International Conference on Availability, Reliability and Security. IEEE, 2015, pp. 417–421.

[2] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer–seller watermarking protocol," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 4, pp. 920–931, 2010.

[3] J. Zhang, Y. Xiang, W. Zhou, L. Ye, and Y. Mu, "Secure image retrieval based on visual content and watermarking protocol," The Computer Journal, vol. 54, no. 10, pp. 1661–1674, 2011.

[4] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 87–96, 2013.

[5] A. Piva, T. Bianchi, and A. De Rosa, "Secure client-side st-dm watermark embedding," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 1, pp. 13–26, 2010.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt. Springer, 2004, pp. 506–522.

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE

Symposium on Security and Privacy. IEEE, 2000, pp. 44–55.
[8] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.
[10] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," Journal of Internet Technology, vol. 16, no. 1, pp. 171–178, 2015.