Received 15 April 2021; Accepted 05 May 2021.

Image Privacy in Social Network Using Invisible Watermarking Techniques

P.Matheswaran[1*], C.Navaneethan[2], S.Meenatchi[3], S.Ananthi[4], K.Janaki[5], A.Manjunathan[6]

[1]Assistant Professor, K.Ramakrishnan College of Technology, Trichy, Tamilnadu, India
[2]Associate Professor, Vellore Institute of Technology, Vellore, Tamilnadu, India
[3]Associate Professor, Vellore Institute of Technology, Vellore, Tamilnadu, India
[4]Assistant Professor, Sri Sairam Institute of Technology, Chennai, Tamilnadu, India
[5]Assistant Professor, M.Kumarasamy College Engineering, Karur, Tamilnadu, India
[6]Assistant Professor, K.Ramakrishnan College of Technology, Trichy, Tamilnadu, India

Abstract

As social media helps to connect with the friends and family, plenty of image data are being uploaded in the site. But the issue to be mentioned with the social media is the data storage. To protect the images from being copied, privacy settings may be enabled as per the individual's choice. However, it is not restricted to stop anyone taking screenshot of the image. Even, as we are aware of the hackers, they may use the images to erase the personal information. Text based encryption, safe storage in the cloud through mobile computing are few instances which will help to maintain our data safely. In addition to the above, this paper aims at incorporating Discrete Wavelet Transform, a new wavelet watermarking application to use the image in a protected format based on a real time application (Facebook). The obtained results will reveal that the proposed technique will protect the image data stored on the server.

Index Terms—Image Processing, Discrete Wavelet Transform (DWT), privacy for images, Watermark, etc.

I. INTRODUCTION

With the wide variety of information technology, digital data has become popular. As it is getting popular, there exists various security threats; hence it is necessary to protect the data from hacks. As a result, image watermarking is one such solution. With the digital watermarking, various goals exist such that, it can verify the owner of the image, and it can identify illegitimate reproduction of the image. This paper concentrates on preventing unauthorized distribution of the image. The implementation of water marking is carried out through the Discrete Wavelet Transform (DWT) image watermarking system for real time image. In the embedding process, the watermark will be encoded into the cover image using a specific location. Various categories of digital watermarking are available. The first category is image watermarking, in which the watermark is embed into image, whereas in the audio and video watermarking, watermark is embed into the audio and video file. Based on the robustness, the watermark is classified into 'fragile', 'semi fragile' and 'robust'. If a digital watermark is "fragile," it can't be detected after even minor changes. If a digital watermark can withstand benign transformations but not malignant transformations, it is said to be semi-fragile. If a digital watermark can withstand a specific set of transformations, it is called robust. Each watermark must meet specific requirements depending on the target application and type. The watermarking scheme's effectiveness is measured by how well it defends against both deliberate and accidental assaults. A watermarking schema has three parts namely, the watermark, encoder and the decoder. The watermarking algorithm plays an effective role by incorporating the watermark into an image. The verification algorithm, on the other hand, verifies the item by evaluating the existence of the watermark and the data bits it contains. To embed the watermark inspired by information coding and image compression, available techniques use various transform domains. Digital watermarks can be visible or invisible depending on how people perceive them. On close inspection, a visible watermark is a secondary translucent mark overlaid on the primary image that can be seen by the viewer. The invisible watermark (which can be either durable or fragile) is embedded in such a way that changes to the pixel value are perceptually undetectable and can only be retrieved through the use of specialized software. This paper concentrates on protecting the privacy of image in social network with the aid of invisible water marking techniques. The robustness property as described above by itself is insufficient to ensure content protection for an invisible watermarking technique. It needs to be created with standard encoder and decoder mechanism. The implementation of the invisible watermarking through Discrete Wavelet Transform (DWT) protects the image on social network by restricting the unauthorized distribution of image. The contribution of the paper is summarized as follows. Section III describes the relevant research works carried out in the domain of image watermarking and section III explains the drawbacks of existing system and finally, section IV encompasses the implementation of watermarking technique followed by the experimental results and conclusion. The results obtained demonstrate the good performance of implemented technique.

II. RELATEDWORK

M. Cheung, J. She, and Z. Jie [1], the paper represents, there are two types of user pairs: linked pairs, which are follower pairs, and nonrelated pairs, which are pairs in which the two users do not have a follower relationship. Centered on user-shared photos, this paper proposes a link discovery process and framework for follower suggestion. BOFT, a functional tool for marking user-shared images, is addressed, with over 360,000 user-shared images labeled with BOFT marks. The features of user-shared images are then investigated and modeled as exponential distributions based on a study of 3 million follower relationships from two social networks of distinct roots, Sky rock and 163 webio, which yielded identical findings. Based on the findings, a realistic follower suggestion scheme is suggested and tested. developed using the discovered relations, which have been thoroughly checked with real-world data It is concluded that follower recommendation is feasible using discovered connections through user exchanged photos, and the recommendation is 60% better than User T and achieves 25% of the efficiency of FOF, a system used when restricted access SGs are available. The discovered relations have also been shown to be capable of determining consumer gender. These discoveries have the potential to have a long-term effect and contribution to scientific science and commercial applications, especially where access to SGs is difficult or limited. This work encourages the use of social network research on any social media platform that has image sharing mechanisms, for example. Many fascinating uses, such as centrality analysis, suggestion, viralized, estimation, among many others, become feasible as a result.

M. Cheung and J. She,.[2] The research looked at 1,598,769 photographs posted by 6,036 users on to log, an image-oriented social network. Based on extensive measurements and characterizations of these user-sharing images, this study established the phenomenon that two users with a higher similarity between their shared images are more likely to collaborate. They are likely to be of the same gender or origin, or to have an online relationship. Based on this phenomenon, an analytic scheme based on bag-of-features tagging is suggested and validated using approximately 1.6 million shared photos to de-anonymize a user's identification using their shared images. It has been discovered that relationship is the most sensitive knowledge for exposing a user's identity. It also includes two showcases were introduced to highlight the efficacy of using user-shared photographs for gender identity and origin inference. The experiments show that using user-shared images to expose user identity is successful. To the best of our understanding, this is the first article to assess how user-generated images can be used to infringe on user privacy and to suggest solutions. A mechanism for resolving user identity by matching posted photos with anonymized profile details and friendships with innovations in wearable technology and mobile devices, posting images on social media has become the standard, so maintaining consumer privacy in shared images will become more relevant. This paper has successfully demonstrated and described the phenomenon that two f users' posted photos are identical, they are more likely to be friends, of the same race, and of the same gender. Since image features are a low-level descriptor, two images of the same attribute vector could be two entirely different images. This may be overcome by integrating other types of attribute vectors, such as color-based or other distributions. It denote various image dimensions such as texture, color, and so on. Aside from using various methods, another difficulty is figuring out how to deal with the billions of images produced every day.

M. Cheung, J. She, and X. Li,,.[3] The paper investigates the use of non-user generated annotation to uncover user relations for follower suggestion. We investigate the use of non-user generated labels with separate colour-based and function-based methods instead of using scale-invariant feature transform (SIFT). The method is validated using a dataset of 542 users and 201006 images, as well as the real relationship between users. made annotation We test a novel approach to non-user produced annotation, using real scraped data relationships with over 200k images; we demonstrate that non-user generated annotation will discover associations for suggestion, independent of the visual methods used to describe images; and we confirm that the feature-based approach is efficient. it outperforms the colour-based and tag-based approaches by 95% and 65%, respectively. To our knowledge, this is first paper to demonstrate that non-user generated annotation is not constrained by the framework used and that feature-based methods are superior for relation discovery. The GIST descriptor was first proposed, and it has yielded positive results for scene categorization and image quest. The aim is to create a low-dimensional, holistic depiction of a scene that does not involve specific segmentation of image regions and artefacts. The system generates feature maps for the image by filtering each pixel with a set of (Gabor) filters. Each feature map is divided into blocks, and the GIST descriptor is calculated by adding the averaged value of each block over all feature maps. The GIST descriptor summarises gradient details (scales and orientations) for various sections of a picture, resulting in a rough definition of the scene.

M. Douze, H. J´egou, H. Sandhawalia, L. Amsaleg, and C. Schmid,.[4] explains about, the global GIST descriptor is compared to the BOF picture representation in a number of scenarios. These explanations have not been compared in a similar environment as far as we know. Obviously, the BOF representation should not be exceeded by the global descriptor. The fixed spatial structure is one of the issues with GIST writing. The layout tests the effect on accuracy due to the fixed segmentation of the spatial image. Finally, we suggested a GIST indexing technique that can increase performance without affecting search accuracy significantly. As compared to the proposed binary code, it has the advantage of requiring only a small portion of the database to be accessed. The plan is to use the GIST descriptor's humming embedding technique as a starting point. This will help you choose the most suitable picture. Then, to enhance the consistency of your placement even more, use filtering and reclassification measures. Two separate applications' GIST descriptors were evaluated and compared to the most recent methods based on local descriptors. When it comes to identifying objects and positions, local representations far outperform global representations. The global GIST descriptor, on the other hand, demonstrates that even massive datasets may find some relevant photos. The GIST descriptor outperforms current native methods for near-duplicate detection due to its high accuracy. Conversions such as resizing, JPEG compression, and selective trimming are particularly well suited. In general, my findings are convincing and can be scaled to very large datasets due to GIST's high performance and low memory use. For GIST descriptors, we also implemented a useful indexing technique. It produces results that are close to those of a general search while being extremely effective.

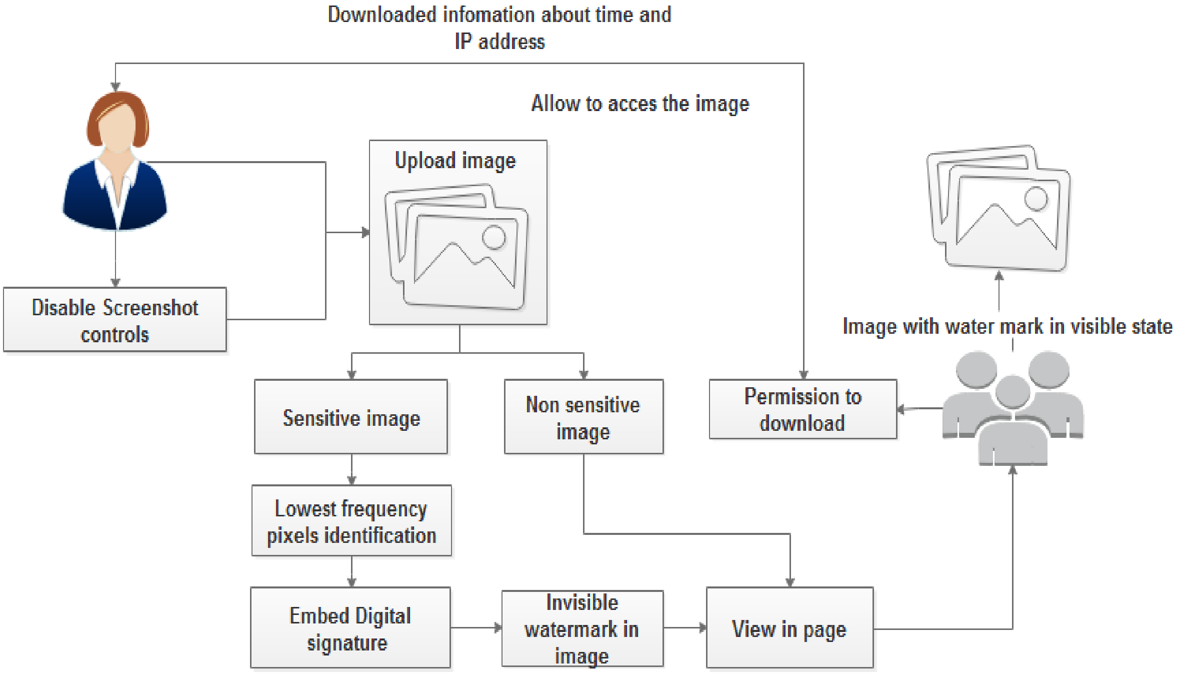
The paper was published by A. Krizhevsky, I. Sutskever, and G. E. Hinton,.[5] The findings show that extensive and deep convolutional neural networks can achieve record results on highly challenging datasets using strictly supervised learning. Surprisingly, the removal of a single convolution layer has an effect on network performance. For example, removing the intermediate level would reduce the first network's output by about 2%. As a result, findings are highly dependent on depth. I didn't use unsupervised pre-training, but I hope it helps to simplify the experiment. While the network has been extended and longer training has been completed, the results have improved, and it can still adapt to the human visual system's time-time course. Finally, for our video sequences, we want to use a very broad and deep convolutional network to provide very useful information when the temporal structure of the still image is lacking or less apparent. The LSVRC-2010 Image Net competition taught convolutional neural networks to rank 101.2 million high-resolution images in a variety of categories. The top 1 and top 5 error rates in the test results are 37.5 percent and 17.0 percent, respectively, which is significantly better than previous state-of-the-art technology.5 convolutional layers, some of which are accompanied by a maximum pooling layer, 3 completely linked layers, and 1000 soft max, make up a neural network with 60 million parameters and 650,000 neurons. Keep going. We used a GPU implementation of unsaturated neurons and convolution calculations to accelerate preparation. We use a newly developed standardised approach called "dropout" to minimise over-adaptation at completely linked layers. It has proven to be extremely effective.

III. EXISTING METHODOLOGIES

Social networking sites have been around for a long time. The Internet is used by people from all disciplines to access various types of knowledge. Furthermore, if confidential information that could be misused by outsiders is revealed, social network security settings would be insufficient. Heuristic attacks are attacks that use known data to extract personal or confidential information. Proposing new hygiene technologies will help to prevent this. Then, to protect your privacy, use a chart-based model and a risk model. Each entity has its own distinct personality. Online users, as first form of individual, may interact with one another and create their own content. This results in the formation of two additional forms of entities. Connections between online users are typically targeted and time sensitive, much like they are in everyday social life. People share pictures of social gatherings, weddings, holidays, and graduations on social media. These photos include you, your family, and those on the Internet, suggesting that these social networking sites are disclosing personal information and breaching privacy. Many video sharing sites offer a range of privacy choices, but these options aren't always sufficient for photos. The explanation for this is mostly due to the amount of data transmitted by the image, as well as the fact that it is unknown if any image processing software was used to process the image or if the image is accurate, the query user can browse through encrypted data sets using searchable encryption (SE) schemes. Automatically recommend policies – Specified by server and fixed policies DCT image quality recognition – Zig Zag scanning approach to deciding image quality.

IV. PROPOSED METHODOLOGIES

Confidentiality, credibility, and reliability are the three primary security features of images in social networks. Only approved personnel should have access to a specific picture, which should be clearly labelled. Consistency indicates that the picture has not been altered by an unauthorised user. Authenticity is a version of an image that can confirm whether it is a photograph of a real person or has been manipulated using different image processing tools. The modulations of these basic functions is growing in tandem with the continued growth and usage of software image editors. Most notably, the widespread use of social media has made posting and exchanging photos incredibly easy. Since these photographs are used as evidence in court and elsewhere, integrity and authenticity are important considerations. It's important to double-check the photos; integrity. After registration, you can usually check to see if the picture has been tampered with. We implemented a watermark method that hides the image's basic pattern in order to understand the image behind the jpeg image. A water level mark can be seen in the picture. Unauthorized users would then only be able to see the watermark data. You may create a watermark that can be restored to a normal image using the inverse DWT Shift the pixel colour of the text content to the pixel colour of the picture in the interface's appearance. As a result, images can be considered irrefutable material. Individuals can set privacy settings to prevent third-party downloads of their photos. As a result, even if the user does not have the most powerful privileges, he or she can easily obtain the watermark information. Then, on the interface system, select the Disable Screen Capture function. Create the social network from the ground up to provide image privacy settings. Use the discrete wavelet transform to post images with watermarks in an invisible state. Disable mouse and keyboard system options unauthorized users only see the watermark during the download process.


Downloaded infomation about time and IP address
Allow to acces the image
Upload image
Disable Screenshot controls
Image with water mark in visible state
Sensitive image
Non sensitive image
Permission to download
Lowest frequency pixels identification
Embed Digital signature
Invisible watermark in image
View in page

.

Fig 4.1 System Architecture

a. SOCIAL NETWORK CREATION

The interaction between people who make, share, and exchange information and ideas in communities and virtual networks is referred to as social networking. This module supports three types of users: image owner, image user, and image server. The image owner will upload the image to the system, which is then stored in the database by the image server. Image users make use of images that the image owner has shared. Enable image owners to use social networking apps as Android apps. Server pages can be made to look like.NET pages.

b. UPLOAD IMAGE

The image acquisition phase is the first step in the sharing method. You can upload a variety of images, including natural and facial images, to this module. Any form and size of picture can be uploaded. The picture is classified as sensitive or non-sensitive in this format. Personal pictures are delicate photographs. A transparent image is an offensive image.

c. EMBEDED THE WATERMARK

In this system the plugin can add watermark text to the images. Watermarks aid in the verification of ownership, the protection of secret content, the prevention of unauthorized copying and dissemination of images over the Internet, and the prevention of digital image tampering. For real-time images, you can use a DWT (Discrete Wavelet Transform) domain image watermark method. During the embedding process, you can use a particular location to encode the watermark on the cover image. The picture is covered by the values in these positions. The OSN homepage receives the watermark image created during the embedding process.

d. PRIVACY SETTING

In our privacy policy, each user's picture is ranked first. The privacy policy for each picture can then be classified and analysed in order to predict the policy. As a result, rather than using the traditional single-step data mining approach to extract image features and strategies, we suggest a two-step method. The two-step approach helps the system to identify policies as having or not having privacy in the first step. The next move is to set up the system without any privacy protections. The user list's extensive details appeal to us.

e. PROTECTION SYSTEM

This module helps you to set up a security or blocking scheme to prevent third-party axes from being used without the image owner's knowledge. This is the method that is used to make the picture private. When a user sets their privacy preferences, all other users are considered third parties. Unauthorized users can only display and use images with this setting. When you download something, you just get the watermark value. Finally, it has a hardware control system that includes screenshot management. Then turn off the screenshot feature. Provides an encryption implementation that extracts system control values while protecting and disables encryption. Any browser can be used to enforce this definition.

Advantages

- Protect the privacy of uploaded images
- Simple to use
- No pre-defined image requirements
- Can be used in a real-time environment.

V. EXPERIMENTAL RESULTS

The suggested algorithm is evaluated in terms of privacy protection and is applied in real-time settings. The findings can be shown using the .NET platform as the front end and SQL SERVER as the back end.

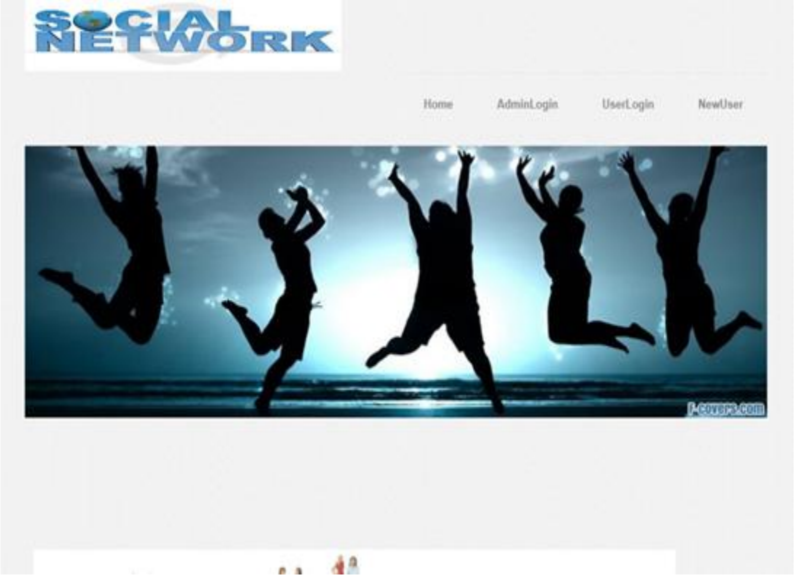
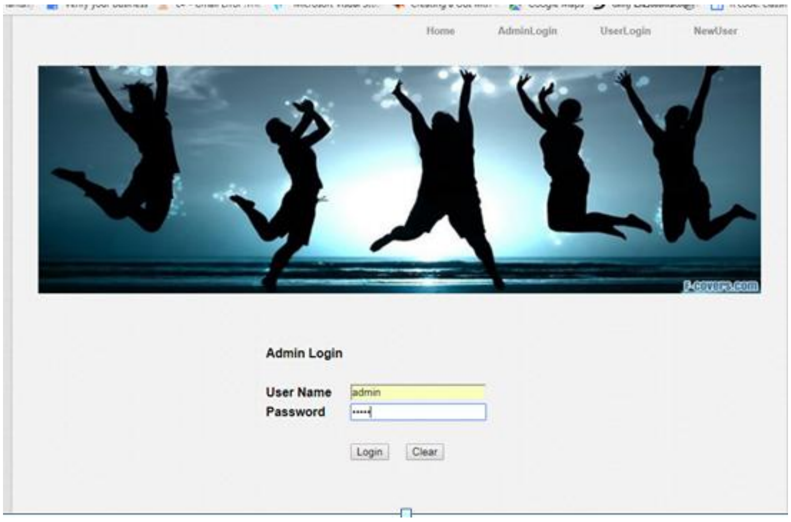


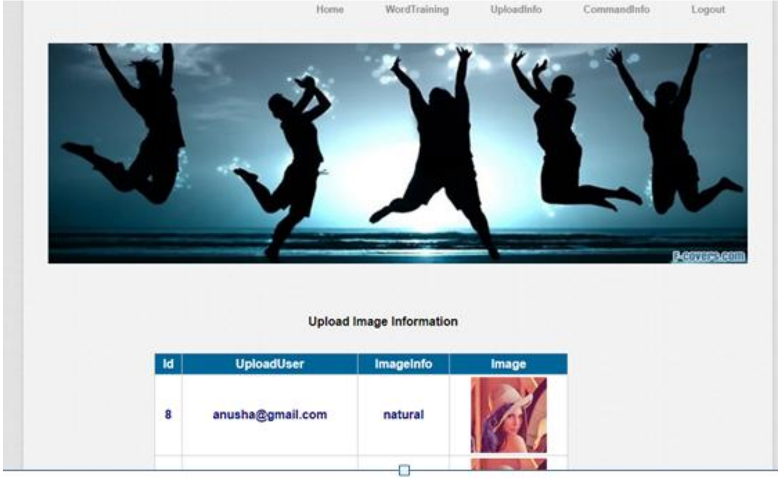
Fig 5.1 Home page



Admin Login

User Name admin
Password •••••

Fig 5.2 Admin Login Page



Upload Image Information

Id	UploadUser	ImageInfo	Image
8	anusha@gmail.com	natural	

Fig 5.3 Upload Image and Information

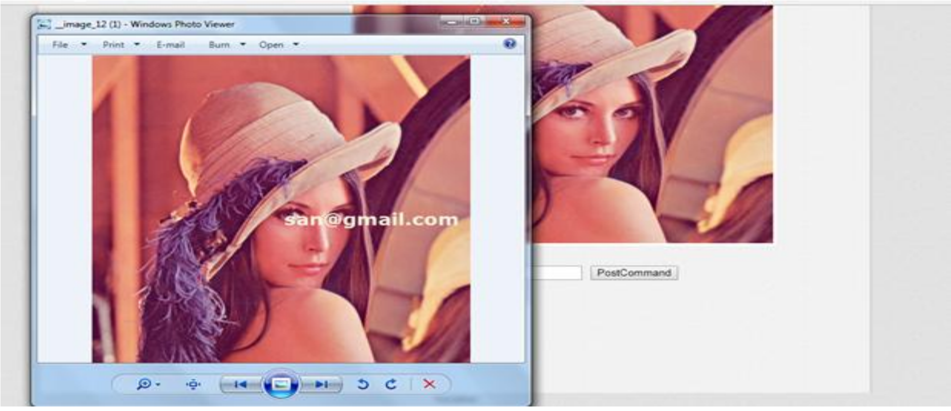


Fig 5.4 Image Displayed with Watermark

VI. CONCLUSION AND FUTURE WORK

The rise of well-known online social networking sites has resulted in a concession of traditional conceptions of privacy, especially in visual media. We provided the architecture, deployment, and assessment in order to promote useful and principled preservation of image privacy on the internet. The digital watermarking method is entirely dependent on the adjustment of DWT coefficients for social purposes. Implemented privacy social network to provide a guard mechanism for user-uploaded images. Original photographs are only accessed by approved persons. Disable the ability to use photographs sent by users. To protect the OSN home page, incorporate cryptographic techniques and various filtering techniques as part of future work. In addition, the work in privacy-based uploaded video content sharing sites will be extended. The findings of the experiment indicated a higher average performance in real time application.

VII. REFERENCES

[1] Xiaojaun Dong, Weiming Zhang, Mohsin Shah, “Watermarking- Based Secure Plaintext Image Protocols for Storage, Show, Deletion and Retrival In the Cloud vol. 13, no. 4, July -August 2020, .

[2] M. Cheung, J. She, and Z. Jie, “Connection discovery using big data of user-shared images in social media,” Multimedia, IEEE Transactions on, vol. 17, no. 9, pp. 1417–1428, 2015.

[3] M. Cheung and J. She, “Evaluating the privacy risk of user-shared images,” ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 12, no. 4s, p. 58, 2016.

[4] M. Cheung, J. She, and X. Li, “Non-user generated annotation on user shared images for connection discovery,” in 2015 IEEE International Conference on Data Science and Data Intensive Systems. IEEE, 2015, pp. 204–209.

[5] M. Douze, H. J´egou, H. Sandhawalia, L. Amsaleg, and C. Schmid, “Evaluation of gist descriptors for web-scale image search,” in Proceedings of the ACM International Conference on Image and Video Retrieval. ACM, 2009, p. 19.

[6] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in Advances in neural information processing systems, 2012, pp. 1097–1105.

[7] K. Chatfield, K. Simonyan, A. Vedaldi, and A. Zisserman, “Return of the devil in the details: Delving deep into convolutional nets,” arXiv preprint arXiv:1405.3531, 2014.

[8] Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell, “Caffe: Convolutional architecture for fast feature embedding,” in Proceedings of the ACM International Conference on Multimedia. ACM, 2014, pp. 675–678.

[9] E. M. Jin, M. Girvan, and M. E. Newman, “Structure of growing social networks,” Physical review E, vol. 64, no. 4, p. 046132, 2001.

[10] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, “Measurement and analysis of online social networks,” in Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. ACM, 2007, pp. 29–42.

[11] X. Liu, B. Qin, R. H. Deng, and Y. Li, “An efficient privacypreserving outsourced computation over public data,” IEEE Trans. Serv. Comput., vol. 10, no. 5, pp. 756-770, 2015.

[12] X. Liu, R. H. Deng, K. K. R. Choo, and J. Weng, “An efficient privacy-preserving outsourced calculation toolkit with multiple keys,” IEEE Trans Inf. Forensics Security, vol. 11, no. 11, pp. 2401- 2414, Nov. 2016.

[13] X. Liu, R. H. Deng, W. Ding, R. Lu, and B. Qin, “Privacy-preserving outsourced calculation on floating point numbers,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2513-2527, Nov. 2016.

[14] X. Liu, R. Choo, R. Deng, R. Lu, and J. Weng, ”Efficient and privacy-preserving outsourced calculation of rational numbers,” IEEE Trans. Depend. Sec. Comput., vol. 15, no. 1, Jan./Feb. 2018.

[15] X. Dong, W. Zhang, M. Shah, B. Wang, and N. Yu, “A restrained paillier cryptosystem and its applications for access control of common secret, oct 2016

[16] S. Al Sharif, F. Iqbal, T. Baker, and A. Khattack, ”White-hat hacking framework for promoting security awareness,” in Proc. 8th IFIP Int. Conf. on New Technologies, Mobility and Security, 2016.

[17] S. Al Sharif, M. Al Ali, N. Al Reqabi, F. Iqbal, T. Baker, and A. Marrington, ”Magec: An image searching tool for detecting forged images in forensic investigation,” in Proc. 8th IFIP Int. Conf. on New Technologies, Mobility and Security, 2016.

[18] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[19] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, ”A DCT-domain system for robust image watermarking,” Signal process., vol. 66, no. 3, pp. 357-372, 1998.

[20] H. W. Lim, S. Tople, P. Saxena, and E. Chang, “Faster secure arithmetic computation using switchable homomorphic encryption,” IACR Cryptol. ePrint Arch. Tech. Rep. 2014/539, Jul. 2014.

[21] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[22] S. Kamara, P. Mohassel, and M. Raykova, “Outsourcing multiparty computation,” IACR Cryptol. ePrint Arch. Tech. Rep. 2011/272, Oct. 2011.

[23] E. Barker, W. Barker, W. Burr,, W. Polk, and M. Smid, ”Recommendation for key management part 1: General (revision 3),” NIST special publication, vol. 800, no. 57, pp. 1-147, 2012.

[24] X. Yan, S. Wang, A. A. A. El-Latif, X. Niu, and Z. Wei, ”A new assessment measure of shadow image quality based on error diffusion techniques,” Journal of Inf. Hiding and Multimedia Signal Process., vol. 4, no. 2, pp. 118-126, 2013.

[25] H. K. Maity and S. P. Maity, “Reversible image watermarking using modified difference expansion,” in Proceedings of the 2012 Third International Conference on Emerging Applications of Information Technology (EAIT), vol. 17, no. 3, pp. 320–323, IEEE, Kolkata, India, November-December 2012

[26] S. L. Lin, C.-F. Huang, M. H. Liou et al., “Improving histogram based reversible information hiding by an optimal weight-based prediction scheme,” Journal of Information Hiding and Multimedia Signal Processing, vol. 1, no. 1, pp. 19–33, 2013.

[27] Indumathi K, Manjunathan A, Balasundhari G, Dharani M, “IoT technology for remote controlled watering system”, International Journal of Engineering Research & Technology, vol.5, issue 13, pp. 1-3,2017.

[28] C Bhuvaneshwari, A Manjunathan, “Reimbursement of sensor nodes and path optimization Materials” Today: Proceedings, 2020.

[29] Bhuvaneshwari C, Manjunathan A, “Advanced gesture recognition system using long-term recurrent convolution network”, Proc. ICONEEEA, 2019 pp. 1-8.

[30] C Bhuvaneshwari, G Saranyadevi, R Vani, A Manjunathan, “Development of High Yield Farming using IoT based UAV”, IOP Conference Series: Materials Science and Engineering 1055 (1), 012007

[31] M Ramkumar, C Ganesh Babu, K Vinoth Kumar, D Hepsiba, A Manjunathan, R Sarath Kumar, “ECG Cardiac arrhythmias Classification using DWT, ICA and MLP Neural Networks”, Journal of Physics: Conference Series, vol.1831, issue.1, pp. 012015.

[32] Z. Zhang, L. Wu, H. Li, H. Lai, and C. Zheng, “Dual watermarking algorithm for medical image,” Journal of Medical Imaging and Health Informatics, vol. 7, no. 3, pp. 607–622, 2017.

[33] H. S. El-sayed, S. F. El-Zoghdy, and O. S. Faragallah, “Adaptive difference expansion-based reversible data hiding scheme for digital images,” Arabian Journal for Science and Engineering, vol. 41, no. 3, pp. 1091–1107, 2016.

[34] Urvoy, D. Goudia, and F. Autrusseau, “Perceptual DFT watermarking with improved detection and robustness to geometrical distortions,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1108–1119, 2014.

[35] A. K. Singh, M. Dave, and A. Mohan, “Wavelet Based Image Watermarking: Futuristic Concepts in Information Security,” Proceedings of the National Academy of Sciences India Section A - Physical Sciences, vol. 84, no. 3, pp. 345–359, 2014