IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

Robust Image Forgery Detection Over Online Social Network Shared Images

Dr. K. Velmurugan[1] and Preethiyangaradevi. A[2], Shalini. S[3]
Head of the Department, Department of Computer Science and Engineering[1]
Student, Department of Computer Science and Engineering[23]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India
csehod@aamec.edu.in[1] and preethipree040622@gmail.com[2],shalini6soundhar@gmail.com[3]

Abstract: *In servers and mobile users, an image is sent over the social network or exchanged. Due to the fact that it contains delicate personal information, the privacy of that data is crucial. A hacker may use social information about a person to discredit them if their image is hacked. Text-based encryption can be used in mobile cloud computing under the current architecture. There are various ways to store data securely utilizing mobile computing, including end-to-end encryption of data transmission and dynamic credential generation that only generates text. We'll be creating a brand-new wavelet watermarking technique called the discrete wavelet transform for use in real-time social network applications like Facebook, and this study suggests an efficient image forgery detection method that recognizes a manipulated foreground or background. Using this technique, images can be used and safely kept on servers. We categorize the image as either common or delicate, and we also enhance the project to include copy right implementation. Run copyright algorithms referred to as wavelet transform algorithms when employing sensitive techniques. After that, provide the receiver secure access to download the pictures. Using C#.NET as the front end and SQL SERVER as the back end, experimental results show the efficiency of current algorithms in real-time social network contexts and a comparison of their privacy rates.*

Keywords: Social Network, Watermarking, Discrete Wavelet Transform.

I. INTRODUCTION

In the modern era, there is an abundance of digital imagery available to us. We used to have complete faith in the truthfulness and integrity of this imagery, but modern technology has eroded that faith. From prestigious publications to the media sector, legal proceedings, retail stores, academic journals, political campaigns, and the photographic satire that lands in our inboxes and on social media. Photographs that have been altered are showing up more frequently. Without a doubt, the authenticity of images is a major concern right now. To confirm the validity of the altered image, there are two basic categories of image forgery detection. The first is an active method, while the second is a passive one, both of which are further discussed in the literature. Two major types of active methods where the real information is added to the digital image are watermarking and steganography. When it's necessary to check the legitimacy of the photograph, the previously saved information is used to shed light. The most common approach to fake an image using passive methods is a copy-move forgery. It involves copying from the image and pasting it back into the original image. There are also alternative quicker methods, like Noise Inconsistency and double JPEG compression. Due to the lossy nature of JPEG (because the majority of photographs are stored in JPEG), both the original and modified image are compressed twice after being processed by photo-editing software. Specific artefacts produced by this double compression differ from those produced by a single compression.

For various purposes, the photos are edited. Some users simply alter the image for fun. Some users purposefully alter the content of the image; this intentional alteration is regarded as malicious attacks like text editing, splicing, and cloning. Many operations that are carried out on images during digital data transfer, such as filtering, compression, boosting, and sharpening, but which leave the image's content or meaning unchanged, are regarded as benign attacks. The photographs are not regarded as trustworthy sources in newspapers, magazines, journals, courts, etc. due to image fabrication. The validity and reliability of these photos must be confirmed. The investigator turned.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

II. RELATED WORK

[1]**Image Forgery Detection**

Numerous forensics techniques have been put forth to confirm the legitimacy of digital photographs, including [2, 3, 5, 7, 8, 18–23, 26, 36, 39, 40]. These techniques look for specific artefacts left behind by processes like splicing [18, 26], copy-move [23, 39], median filtering [8, 20], inpainting [21, 22, 36], etc. to identify the faked regions. To address the issue of detecting generic (compound) forms of forgeries, an increasing number of approaches have been developed [4,5,11,12,27,37,41,42], among which deep learning based methods are the most effective. In this vein, Wu et al.'s [37] universal forgery detection network, the MT-Net, was proposed. It initially extracts image alteration features before identifying anomalous regions. The forensic similarity to detect whether two images are comparable was recently presented by Mayer and Stamm [27].To assess whether two image patches contain the same forensic evidence, Mayer and Stamm [27] recently introduced the forensic similarity. Cozzolino and Verdoliva [12] developed a method for extracting a camera model fingerprint, known as noiseprint, in order to reveal the forged regions from the viewpoint of the camera fingerprint. Zhuang et al.'s [42] training data creation method for discovering the signs of generic forgeries made use of Photoshop scripting.

[2] **Online Social Network (OSN)**

The widespread use of OSN platforms like Facebook, Wechat, Weibo, and others has made it much easier to share and disseminate photographs. However, practically all OSNs alter the uploaded photos in a lossy manner, as shown by numerous existing works [33, 34]. The noise generated by these lossy activities may significantly reduce the efficacy of forensic techniques. As shown in [32-34], using Facebook as an example, these changes primarily involve three steps: scaling, enhancement filtering, and JPEG compression. Resizing would be done specifically if the image resolution was higher than 2048 pixels. The image is then subjected to a very adaptable and intricate enhanced filtering process on a few chosen blocks. Due to their complexity, as indicated in [33, 34], it is very difficult to exactly know these enhanced filtering methods. The image is then subjected to a round of JPEG compression with an adjustable quality factor (QF) based on the image content. The QF values utilized by Facebook range from 71 to 95, according to the examination of the dataset presented in [33]. Although there are differences between the picture alterations performed on various OSN platforms, the operations carried out by popular OSNs nevertheless have many similarities (such as the widely used JPEG compression) [33]. A few forensic techniques already in use [9, 24, 38] aim to pinpoint the implicated transmission processes. The first feature decoupling approach for the identification of two operations based on blind signal separation was proposed by Liao et al. [9, 24]. You et al. [38] suggested a method by creatively expressing the manipulation chain detection as a long chain to further highlight it.

[3] **Discrete Wavelet Transform**

A mathematical method for the hierarchical breakdown of a picture is the discrete wavelet transform (DWT). The transformation is based on breaking down a signal into wavelets, which are brief waves with variable frequencies. An original signal is divided up into wavelet transform coefficients by the wavelet characteristics, and these coefficients carry positional data. When these coefficients are subjected to an inverse wavelet transformation, the original signal can be fully recreated.

[4] **Copy-Move Image Forgery Detection**

Due to the availability of sophisticated editing tools and fully functional digital cameras, region duplication in picture forgeries has become widespread. The majority of current block-based copy-move detection methods have trouble spotting such manipulation when postprocessing processes like scaling and JPEG compression are used. In this article, a copy-move picture fraud detection system is proposed that makes use of center-symmetric local binary patterns (CSLBP) and Hessian characteristics. Four steps make up the suggested method: (1) detecting the item using normalized cut segmentation, (2) localizing the local interest points of each object using the Hessian method, (3) obtaining CSLBP features, and (4) identifying duplicated regions in forgeries. The approach is resistant to post-processed copy-move forgeries under scaling and JPEG compression, according to the findings of the experiments.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

[5]**Watermark for Tamper Detection and Localization**

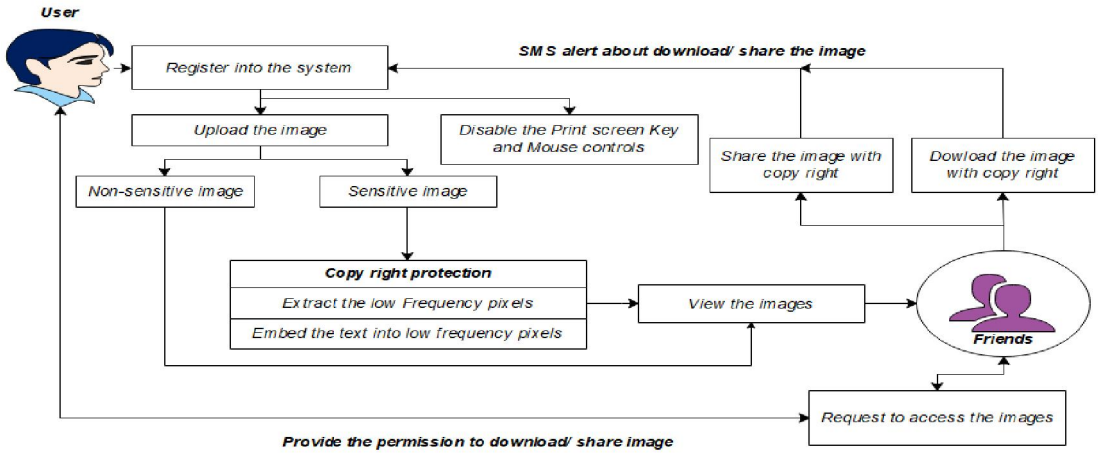
Data security has grown to be a significant current concern. The integrity of image data is said to be protected by digital image watermarking. Watermarking algorithms are able to identify several types of attacks on photos. In this work, a reliable watermarking method for fragile images is suggested. The suggested watermarking algorithm seeks to identify and pinpoint picture manipulation. Block-based embedding in the spatial domain is the recommended approach. It introduces the use of SHA-1 (Secure Hashing Algorithm) hashing to include a unique key-based encryption. High PSNR and SSIM are present in the watermarked photos. The program can handle tampering of all sizes, from extremely small to very enormous. The suggested method has been examined for numerous tampering attempts, including copy-paste, copy-move, constant average, and general tampering.

III. WORKING

Install Visual Studio and get the best bundle for devices implementing C# code by downloading and installing it.
Modern, object-oriented, and type-safe programming languages like C# are available. With C#, programmers may create a wide variety of.NET-compatible apps that are secure and reliable. Programmers who are familiar with C, C++, Java, and JavaScript will feel immediately at home with C# due to its roots in the C family of languages.
A summary of the working procedure is provided below:

1. Putting the Visual Studio platform into place.
2. Establishing a social network for the upload and storage of photographs. Any style or size of image is acceptable.
3. Incorporating the watermark into the image and applying the discrete wavelet transform technique.
4. Set the privacy with or without protection, and then look for any suspicious behaviour or activity.
5. Disabling mouse and print screen functions.

IV. SYSTEM MODEL



V. METHODOLOGY

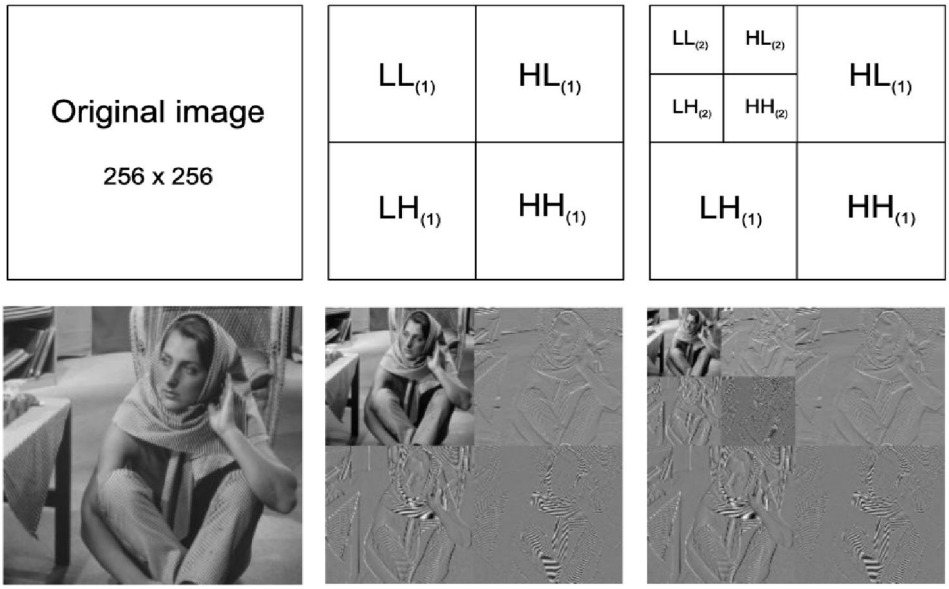
This watermarking approach, which uses Discrete Wavelet Transform to embed the watermark in an image, is the basis for the identification of picture forgeries. This technology deters the unlicensed copying and dissemination of images over the Internet.

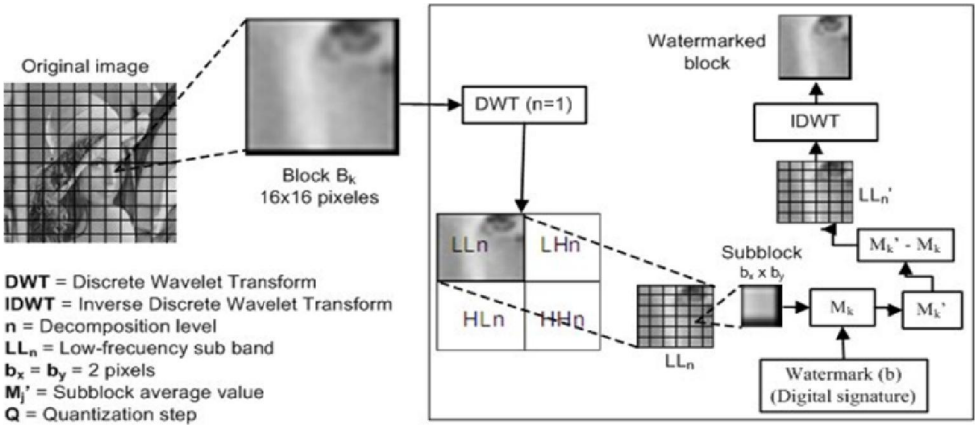
5.1 Discrete Wavelet Transform

In common with other wavelet transforms, it is any wavelet transform for which the wavelets are discretely sampled. Like other wavelet transforms, it has a significant benefit over Fourier transforms in that it can capture both frequency and location information.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

- DWT divides a picture into three details, one approximation, and two subimages or subbands. LL, LH, HL, and HH are the bands.
- Low frequencies can be found in LL both horizontally and vertically. High frequencies can be found in HH in both the horizontal and vertical directions. High frequencies are present in both the horizontal and vertical directions in HL. High frequencies are present vertically and low frequencies are present horizontally in LH.
- Since the high frequency detail bands (LH, HL, and HH) are less sensitive to human vision, watermarks can be incorporated into these areas. The robustness of the watermark is increased by embedding into these areas without degrading the image's quality further.





5.2 Watermark Embedding

- In this procedure, the cover picture is subjected to 2D DWT, which divides the image into four sub-bands: low frequency approximation, high frequency diagonal, low frequency horizontal, and low frequency vertical. The watermark image, which must be incorporated into the cover image, is subjected to a similar 2D DWT procedure.
- Alpha blending is the method used to apply a watermark. The watermark and cover image's separated parts are further multiplied by a specific scale factor and appended. The cover picture should be larger than the watermark while embedding, but the frame sizes of the two images should be the same.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

- The watermark image is created using the alpha blending technique as follows: WMI= k*(LL1) + q*(WM1). Where WMI stands for "watermarked image," LL1 for "low frequency approximation of the original image," WM1 for "watermark," and k and q for the corresponding scaling factors for the original and watermark. The final safe watermarked image is created by applying an inverse discrete wavelet transform to the coefficient of the watermarked image. Process of embedding a watermark, Watermark Removal The steps used in the embedding process are used in this method in the opposite order. Both the cover picture and the watermarked image are subjected to the first discrete wavelet transform. After that, an alpha blending technique is used to recover the watermark from the watermarked image.
- The alpha blending method RW= (WMI - k*LL1) is the alpha blending formula used to extract watermarks. Where WMI stands for watermarked image, LL1 for low frequency approximation of the original picture, and RW for recovered watermark. The final watermark extraction image is created by performing an inverse discrete wavelet transform on the coefficient of the watermark picture.

VI. CONCLUSION

- Implemented privacy social network to provide guard system to images which are uploaded by users.
- Only authorized person can get original images.
- Disable the possibilities to use images which are posted by users.
- Block the unwanted messages from user home pages

REFERENCES

[1]. S.Saravana Kumar, R.Barath, Mrs.A.G.JessyNirmal, "COPY MOVE FORGERY IMAGE DETECTION" International Journal of Advanced Research in Computer Science Engineering and Information Technology Volume: 4, Issue: 3, Special Issue: 2.

[2]. BarnaliSarma, Gypsy Nandi, "A Study on Digital Image Forgery Detection" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11.

[3]. Reshma Raj, Niya Joseph, "Keypoint extraction using SURF algorithm for CMFD" Science Direct Procedia Computer science93, 6th International Conference on Advances in Computing & Communications, ICACC.

[4]. Hany, F. Image forgery detection. IEEE Signal Process Mag. 2009, 26, 16–25.

[5]. Yousif, S.F.; Abboud, A.J.; Radhi, H.Y. Robust image encryption with scanning technology, the El-Gamal algorithm and chaos theory. IEEE Access 2020, 8, 155184–155209.

[6]. Gul, E.; Ozturk, S. A novel hash function based fragile watermarking method for image integrity. Multimed.Tools. Appl. 2019, 78, 17701–17718.

[7]. Gull, S.; Loan, N.A.; Parah, S.A.; Sheikh, J.A.; Bhat, G.M. An efficient watermarking technique for tamper detection and localization of medical images. J. Ambient Intell. Humaniz.Comput. 2020, 11, 1799–1808

[8]. Bhalerao, S.; Ansari, I.A.; Kumar, A. A secure image watermarking for tamper detection and localization. J. Ambient Intell. Humaniz.Comput. 2021, 12, 1057–1068.

[9]. Gardella, M.; Musé, P.; Morel, J.M.; Colom, M. Forgery Detection in Digital Images by Multi-Scale Noise Estimation. J. Imaging. 2021, 7, 119.

[10]. Kumar, C.; Singh, A.K.; Kumar, P. A recent survey on image watermarking techniques and its application in e-governance.Multimed.Tools. Appl. 2018, 77, 3597–3622.

[11]. Abboud, A.J.; Jassim, S.A. Biometric templates selection and update using quality measures. In Mobile Multimedia/Image Processing, Security, and Applications 2012; SPIE: New York, NY, USA, 2012; Volume 8406, p. 840609

[12]. Amiri, T.; Moghaddam, M.E. A new visual cryptography based watermarking scheme using DWT and SIFT for multiple cover images. Multimed.Tools. Appl. 2016, 75, 8527–8543.

[13]. MaddumaBuddhika, and Sheela Ramanna. "Content-based image authentication framework with semi-fragile hybrid watermark scheme." Man-Machine Interactions 2.Springer Berlin Heidelberg, 2011.239-247.