ICEST-2K24 [International Conference on Engineering, Science and Technology]
In Association with
International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN - 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Result Paper on JPEG Vigilant : AI-Powered Malware Image Detection

Prof. Jalindar N. Ekatpure[1], Mr. Kharade Nilesh Shahaji[2], Mr. Kshirsagar Dipak Vinod[2], Mr. Mind Rushikesh Satish[2], Mr. Korake Digvijay Dilip[2]

[*1]Assistant Professor, S. B. Patil College of Engineering, Indapur, Maharashtra, India

[2]S. B. Patil College of Engineering, Indapur, Maharashtra, India

ABSTRACT

The biggest invention of 21st century is the social media. It is biggest platform which is using to share data, files and documents. Even it is using to share thoughts, ideas and feelings using different tools and techniques. People are hyper connected with each other and they are continuously sharing the information. For criminals, deploying malware in such scenario is very easy and propagating malware through JPEG images and QR Code is one of the best and most advanced method. Using steganography techniques, criminals embedded the malicious codes with legitimate or innocent looking images. This malicious content is just few line of codes which exploit the vulnerability of application. It gives remote access of this system to the attacker which can do criminal act. In this framework, our primary purpose is to find the presence of any code or data in image. After it, the major section of this framework based upon the finding of code and its adverse effects. This framework shows the corresponding solution to the malicious code presence in JPEG images and QR code which are spreading through online social networking sites.

Keywords: JPEG, image, QR, malware detection, machine learning, features

I. INTRODUCTION

With the growing popularity of the Internet, computer systems and the internet become increasingly ubiquitous, which make the internet capable devices into a hyper connected world. One side of this transformation facilitate the user other side it impede from unstructured and sporadic attacks to well thought-out controlled organized attacks. Previously the attacks used the conventional methods to infect its victim, where the primary intent is a seek for fame. Now, it is well organized multi-vector attack on a global scale, where the primary objective is financial profits. The new battlefield for cybercrime is now Online social Networks (OSNs), which provide a new, prolific, unexplored and upbringing environment for the dissemination of malwares over the cyberspace. This new online social networks or social dimension act as challenges in fighting web based crime: (a) the techniques engaged by attacker/hackers are relentlessly evolving, and (b) the worldwide public is uninformed, credulous and easily enticed into suspicious websites or clicking on distrustful content i.e. installing apps with the lure of fake and false rewards. For a non-technical crowd who are using social media innocently are trapped unintentionally into these types of attacks. According to

Internet Security Threat Report - Symantec Report, there is increase of 125% in cybercrime in year 2016 compare to 2015. Beyond this nuisance, these types of social malware resulting a loss of real money for users.

II. LITERATURE SURVEY

In this paper[1], a watermarking algorithm of color image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD). First convert host color image from RGB color space to YUV color space. Then a layer of discrete wavelet transform is applied to the luminance component Y, and divided the low frequency and into blocks by using discrete cosine transform, and conducted SVD with every block. Finally embed watermark to the cover image.

In this paper[2], a new digital watermarking model is proposed for the medical images. An improved SMQT is used for image enhancement and the image is being segmented using OTSU thresholding. Discrete Wavelet Transform (DWT) and Inverse DWT are used to embed and extract the watermark on the host image. The goal of our scheme is to make the water marking more robust against attacks and secure the image from privacy threats.

This paper[3] presents a Wave let trans form Singular Value Decomposition based robust zero water marking technique for medical images to address the privacy and security issues. Unlike conventional water marking, the proposed method conserves the reliability of the cover image without bringing any artifacts and without any change in the critical information contained in the medical image. The performance of the scheme is assessed with tele ophthalmological images. The simulation results reveal the robustness of the proposed technique against various image processing attacks and indicate its suitability for safe exchange of medical images among remote medical practitioners.

This research[4] is done to find the best digital water marking technique to highly secure digital image form the illegal copies. The research work also denationalize the possibilities of dual watermarking. Various standard research articles were studied and it is found that dual watermarking is possible with some situation. This research work motivates and offers different combinations on digital watermarking techniques in near future for efficient output of watermarking.

The paper [5] proves that the contrast of XVCS is 2((k-1)) times greater than OVCS. The monotone property of OR operation degrades the visual quality of reconstructed image for OR-based VCS (OVCS). Accordingly, XOR-based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast. Advantages are: Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages are: Proposed algorithm is more complicated.

In [6] paper, present a blind, key based watermarking technique, which embeds a transformed binary form of the watermark data into the DWT domain of the cover image and uses a unique image code for the detection of image distortion. The QR code is embedded into the attack resistant HH component of 1stlevel DWT domain of the cover image and to detect malicious interference by an attacker. Advantages are: More information representation per bit change combined with error correction capabilities. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks. Disadvantages are: Limited to a LSB bit in the spatial domain of the image intensity values. Since the spatial domain is more susceptible to attacks this cannot be used.

In [7] paper, design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in that it uses the QR

characteristics to achieve secret sharing and can resist the print-and-scan operation. Advantages are: Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. Disadvantages are: Need to improve the security of the QR barcode. QR technique requires reducing the modifications.

The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication [8]. Paper innovates plant species classification using Deep Learning and leaf vein features, aiming to automate identification, accelerate research, aid conservation, and foster education in botany and technology.[14] The public level is the same as the standard QR code storage level; therefore, it is readable by any classical QR code application. Real-time face detection and recognition achieved through Viola-Jones method. Software captures images, stores in database. Automated system detects person using three-phase methodology.[13] The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using qr code with an error correction capacity. Advantages are: It increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the P&S process. Disadvantages are: Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.

To protect the sensitive data, [9] paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones. For a normal scanner, a browser can only reveal the formal information from the marked QR code. Advantages are: The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography. Only the authorized user with the private key can further reveal the concealed secret successfully. Disadvantages are: Need to increase the security. As per paper [11] authors had explained about identification of various harmful URLs through use of Machine Learning techniques.

III.PROPOSED SYSTEM

A. Problem Statement

To build and implement web application for MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images

B. Architecture Diagram

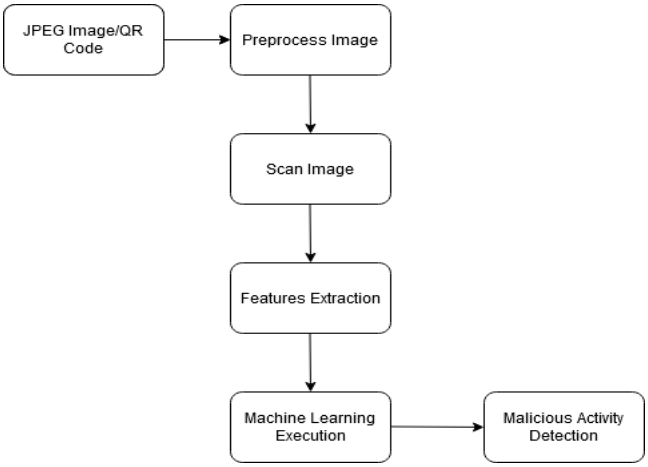

Figure 1: Architecture Diagram

C. Requirements

1) Hardware Requirements:

- Processor- Intel i5/i7
- Speed- 3.1 GHz
- RAM- 8 GB(min)
- Hard Disk- 50 GB

2) Software Requirements

- Operating System- Windows
- Language- Python
- IDE- VS code

D. Work Flow Of System

- This malicious content is just few line of codes which exploit the vulnerability of application.
- It give remote access of this system to the attacker which can do criminal act.
- In this framework, our primary purpose is to find the presence of any code or data in image. After it, the major section of this framework based upon the finding of code and its adverse effects.
- This framework show the corresponding solution to the malicious code presence in JPEG images which are spreading through online social networking sites.

IV. ALGORITHM

The structure of CNN algorithm includes two layers. First is the extraction layer of features in which each neuron's input is directly connected to its previous layer's local ready fields and local features are extracted. The spatial relationship between it and other features will be shown once those local features are extracted. The other layer is feature_map layer; Every feature map in this layer is a plane, the weight of the neurons in one plane are same. The feature plan"s structure make use of the function called sigmoid. This function known as activation function of the CNN, which makes the feature map have shift indifference. In the CNN each convolution layer is come after a computing layer and it's usage is to find the local average as well as the second extract; this extraction of two feature is unique structure which decreases the resolution.

Step1: Select the dataset.
Step2: Perform feature selection using information gain and ranking
Step3: Apply Classification algorithm CNN
Step4: Calculate each Feature fx value of input layer
Step5: Calculate bias class of each feature
Step6: The feature map is produced and it goes to forward pass input layer
Step7: Calculate the convolution cores in a feature pattern
Step8: Produce sub sample layer and feature value.
Step9: Input deviation of the kth neuron in output layer is Back propagated.
Step10: Finally give the selected feature and classification results.

V. RESULT DISCUSSION

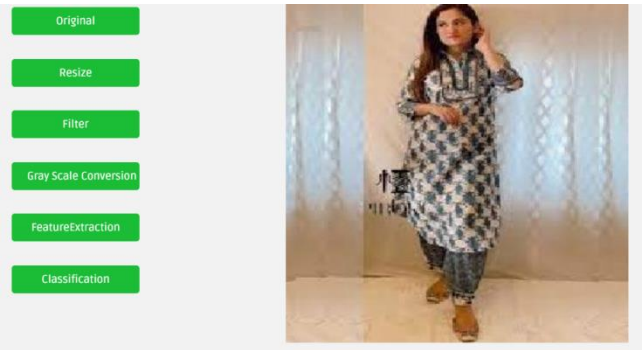

Figure 2:

Figure 3:

VI. CONCLUSION

In this paper, we present MalJPEG, a machine learning based solution for efficient detection of unknown malicious JPEG images. To the best of our knowledge, we are the first to present a machine learning-based solution tailored specifically for the detection of malicious JPEG images. MalJPEG extracts 10 simple but discriminative features from the JPEG file structure and leverages them with a machine learning classifier, in order to discriminate between benign and malicious JPEG images.

VII. REFERENCES

[1]. C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.

[2]. P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code," AEU - International Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074-1084, 2015.

[3]. P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.

[4]. I. Tkachenko, W. Puech, C. Destruel, et al., "Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.

[5]. P. Y. Lin, Y. H. Chen, "High payload secret hiding technology for QR codes," Eurasip Journal on Image & Video Processing, vol. 2017, no. 1, pp. 14, 2017.

[6]. F. Liu, Guo T: Privacy protection display implementation method based on visual passwords. CN Patent App. CN 201410542752, 2015.

[7]. S J Shyu, M C Chen, "Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures," IEEE Transactions on Circuits & Systems for Video Technology, vol. 25, no. 9, pp.1-1,2015.

[8]. H. D. Yuan, "Secret sharing with multi-cover adaptive steganography," Information Sciences, vol. 254, pp. 197–212, 2014.

[9]. J. Weir, W. Q. Yan, "Authenticating Visual Cryptography Shares Using 2D Barcodes," in Digital Forensics and Watermarking. Berlin, German: Springer Berlin Heidelberg, 2011, pp. 196-210.

[10]. G. Wang, F. Liu, W. Q. Yan, "2D Barcodes for visual cryptography," Multimedia Tools and Applications, vol. 2, pp. 1-19, 2016.

[11]. Karve, S. M, Kakad, S, Swapnaja Amol, Gavali, A. B., Gavali, S. B.., & Shirkande, S. T. (2024). An Identification and Analysis of Harmful URLs through the Application of Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 12(17s), 456–468. https://www.ijisae.org/index.php/IJISAE/article/view/4905

[12]. Nalawade, V. S., Ashok, G. K., Hanumant, B. A., &Reshma, G. (2021). ENCRYPTION THEN COMPRESSION BASED SYSTEM USING GRAYSCALE BASED IMAGE ENCRYPTION FOR JPEG IMAGES.

[13]. Ekatpure, J., Nair, D., Deshpande, M., Sagare, S., & Jadhav, P. (2021). ATM Security Using Image Processing in Machine Learning. International Research Journal of Innovations in Engineering and Technology, 5(6), 29.

[14]. Ekatpure, J. N., Kamble, Y. P., More, P. T., & Patankar, S. S. (2023). A Survey On Leaf Vein Morphometrics: A Deep Learning Approach to Plant Classification.