(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :22/02/2024

(21) Application No.202441012662 A
(43) Publication Date : 08/03/2024

(54) Title of the invention : MALWARE CLASSIFICATION USING ORTHOGONAL MOMENTS: A NOVEL TECHNIQUE.

(51) International classification :G06K0009620000, G06F0021560000, G06N0020100000, G06N0003020000, G06F0017140000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Chandra Mohan Bhuma
Address of Applicant :B.Chandra Mohan Department of ECE Bapatla Engineering College Bapatla - 522102 ---------- ----------
2)Tatikonda Krishna Chaitanya
3)Challa Naga Raju
4)K. Sambasiva Rao
5)P. Surendra Kumar
6)Dasari Swetha
7)Bapatla Engineering College
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Chandra Mohan Bhuma
Address of Applicant :B.Chandra Mohan Department of ECE Bapatla Engineering College Bapatla - 522102 ---------- ----------
2)Tatikonda Krishna Chaitanya
Address of Applicant :Asst. Professor, Department of Electronics and Communication Engineering, Bapatla Engineering College, Bapatla 522102, Andhra Pradesh, India Bapatla ---------- ----------
3)Challa Naga Raju
Address of Applicant :Asst. Professor, Department of Electronics and Communication Engineering, Bapatla Engineering College, Bapatla 522102, Andhra Pradesh, India Bapatla ---------- ----------
4)K. Sambasiva Rao
Address of Applicant :Assoc. Professor, Department of Electronics and Communication Engineering, Bapatla Engineering College, Bapatla 522102, Andhra Pradesh, India Bapatla ---------- ----------
5)P. Surendra Kumar
Address of Applicant :Assoc. Professor, Department of Electronics and Communication Engineering, Bapatla Engineering College, Bapatla 522102, Andhra Pradesh, India Bapatla ---------- ----------
6)Dasari Swetha
Address of Applicant :Asst. Professor, Department of Electronics and Communication Engineering, Bapatla Engineering College, Bapatla 522102, Andhra Pradesh, India Bapatla ---------- ----------
7)Bapatla Engineering College
Address of Applicant :Bapatla Engineering College, Bapatla Andhra Pradesh, India 522102 Bapatla ---------- ----------

(57) Abstract :
This work addresses the problem of malware classification using orthogonal moments. Malicious programs for attacking and gaining access to sensitive and valuable information are growing at an alarming rate. New malware files are being introduced by the attackers daily. Hacking, spoofing, phishing, and spyware are becoming common even in mobile transactions. It is becoming a challenging task for cybersecurity professionals. An approach gaining attention in recent times is to convert the malware binaries into RGB color images and apply deep learning algorithms. In this work, a malware classification algorithm using Orthogonal Moments is proposed. Orthogonal moments are able to represent the image content in a more compact form. Several orthogonal moments are available in the literature. Zernike Moments (ZM), Pseudo-Zernike Moments (PZM), Orthogonal Fourier-Mellin Moments(OFMM), Chebychev-Fourier Moments(CFMM), Pseudo Jacobi-Fourier Moments (PJFM), and Jacobi-Fourier Moments (JFM) utilize Jacobi Polynomials. By using harmonic functions, Radial Harmonic Fourier Moments (RHFM), Exponent-Fourier Moments (EFM), Polar Complex Exponential Transform (PCET), Polar Cosine Transform (PCT), and Polar Sine Transform (PST) have been developed. Moments based on Eigen functions are less. Bessel-Fourier Moments (BFM) is one under this category. In addition, Hahn Moments, Gegenbauer Moments, Charlier Moments, Racah Moments, and Gaussian Hermite Moments have been used in pattern recognition, classification, and retrieval. In this work, the image moment is computed for the images of the malware dataset. The image moments (features) are applied to a Linear Support Vector Machine classifier for classifying the 25 malware classes from the Malimg dataset which contains 9339 images in total. It is an imbalanced dataset. A pool of feature matrices is computed from various moments (17 types of moments) by varying the order and some parameters of a particular moment category. Further, the selected features/moments are concatenated from the pool to improve the classification accuracy. The classification metrics i.e., accuracy, balanced accuracy, F1 score, precision, and recall are reported to justify the effectiveness of the proposed algorithm. With a 3 fold-stratified train test split, the classification accuracy is more than 97.5% with a balanced accuracy over 95% and is superior to the many existing algorithms in the literature. Pattern recognition and computer vision both heavily rely on image representation. It is essential to many programs that aim to comprehend visual content. Moment-based image representation has proven to be useful in meeting the fundamental requirements of semantic description because of its advantageous mathematical characteristics, particularly its geometric independence and invariance. This work provides a novel technique for malware image classification, addressing recent developments in image moments and their applicability in image classification.

No. of Pages : 33 No. of Claims : 3