# Image Splicing Detection Using Generalized Whittaker Function Descriptor

**Dumitru Baleanu[1,2,3], Ahmad Sami Al-Shamayleh[4] and Rabha W. Ibrahim[5,*]**

[1]Department of Mathematics, Cankaya University, Ankara, 06530, Turkey
[2]Institute of Space Sciences, Magurele-Bucharest, R76900, Romania
[3]Department of Medical Research, China Medical University, 40402, Taiwan
[4]Department of Networks & Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Al-Salt, Amman, 19328, Jordan
[5]Near East University, Mathematics Research Center, Department of Mathematics, Near East Boulevard, PC: 99138, Nicosia /Mersin 10 – Turkey
*Corresponding Author: Rabha W. Ibrahim. Email: rabhaibrahim@yahoo.com
Received: 26 October 2022; Accepted: 29 December 2022

**Abstract:** Image forgery is a crucial part of the transmission of misinformation, which may be illegal in some jurisdictions. The powerful image editing software has made it nearly impossible to detect altered images with the naked eye. Images must be protected against attempts to manipulate them. Image authentication methods have gained popularity because of their use in multimedia and multimedia networking applications. Attempts were made to address the consequences of image forgeries by creating algorithms for identifying altered images. Because image tampering detection targets processing techniques such as object removal or addition, identifying altered images remains a major challenge in research. In this study, a novel image texture feature extraction model based on the generalized k-symbol Whittaker function (GKSWF) is proposed for better image forgery detection. The proposed method is divided into two stages. The first stage involves feature extraction using the proposed GKSWF model, followed by classification using the "support vector machine" (SVM) to distinguish between authentic and manipulated images. Each extracted feature from an input image is saved in the features database for use in image splicing detection. The proposed GKSWF as a feature extraction model is intended to extract clues of tampering texture details based on the probability of image pixel. When tested on publicly available image dataset "CASIA" v2.0 (Chinese Academy of Sciences, Institute of Automation), the proposed model had a 98.60% accuracy rate on the YCbCr (luminance (Y), chroma blue (Cb) and chroma red (Cr)) color spaces in image block size of $8 \times 8$ pixels. The proposed image authentication model shows great accuracy with a relatively modest dimension feature size, supporting the benefit of utilizing the k-symbol Whittaker function in image authentication algorithms.

**Keywords:** Image forgery; image authentication; fractional calculus; k-symbol; Whittaker function; texture features; SVM

## 1  Introduction

The key reason for image authentication is the growing number of fake images that are presented as realistic interpretations of real-life results but then are later proven to be fakes. Image authentication systems seek to confirm the data accuracy, either positively or negatively. With the simplicity of use of image editing software, image manipulation has become common in the digital age. With the advancement of digital image editing tools, it is now easier than ever to alter the content of images and spread them across a broad range of cyberspace. Because of the advanced editing tools that are easily available and simple to use, image manipulation detection has become a hot research subject in image processing in recent years. As a result, image manipulation has increased to the point where it is difficult to distinguish between original and manipulated images with the human eye. With the massive increase and the use of digital cameras, it is critical to authenticate the digital material, particularly if it is to be utilized as proof in the courts [1]. As a result, image forensics tools can use image content to check the integrity of digital media material. Visual forensics are the detection and analysis of image attributes that may indicate the image's authenticity [2]. Since the development of image manipulation software, identifying manipulated images has been considered as the key issue in image authentication research. The classification of image forgery detection approaches is shown in Fig. 1.
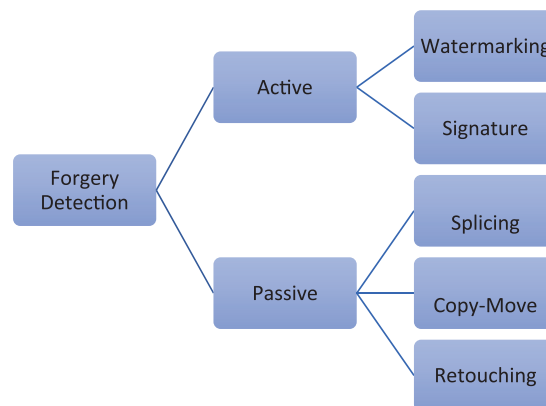


**Figure 1:** Illustration of image forgery detection approaches

Image manipulation can be classified into two approaches in general. When an image is made using the active technique, a watermark or digital signature is inserted. Because there is no extra information for image forgery detection in the passive technique, it is also known as the blind approach. This method is based on features derived directly from images. Image tampering is the technique of replacing an original image with one or more new ones. If the original image's content is replaced by new content from the same image, the process is known as copy-move; if the original image's content is replaced by new material from another image, the process is known as image splicing [3,4]. Image cloning (or copy-move) and image splicing are the two general forms of image forgeries. Image tampering usually leaves no visible clues as to whether the image has been tampered with or not; however, some image statistics may be altered.

Many ways have been proposed and are still being developed to detect the two most common forgeries, which can be utilized to prevent additional damage. Image splicing, as opposed to copy-move forgery, is the act of including mixing and merging pieces from other images to create a composite fabricated image, as seen in Fig. 2A. The insertion of the spliced portion from another image will result in a disrupted pattern that seems like irregularities across the image. For example, the texture of an

image may get warped because of the splicing action. Because texture is mathematical descriptions of image attributes, texture features can be used to detect splice tampering. Fig. 2B depicts how the splicing process distorts the image texture. The motivation for proposing an image authentication based on image forgery detection is because textural properties are immediately altered by the splicing process, offering a numerical basis for distinguishing between authentic and forged images.



Original Image          A-Splices region          B-Spliced Image

**Figure 2:** Illustration of image forgery (splicing)

Because image forgery is a binary situation–either authentic (original) or tampered (forged), it may be automatically identified using machine learning classification algorithms. As image fabrication has increased, forgery detection systems with more advanced algorithms have been presented recently.

Varied works using enhanced detection methodologies have been published in the literature under various forged image conditions. There are certain limitations in these studies, such as a lack of statistical detail for feature extraction, namely on forged image areas. The key to developing the image features model is to determine how to extract the image's principal features. The extraction of major image features, as well as the type of features extracted, are crucial aspects of image authentication. The main objective of this study is to extract the texture features for a better image forgery detection by using generalized k-symbol Whittaker function (GKSWF)-based feature extraction algorithm. The proposed work will be used to achieve better image forgery detection using the YCbCr image color space.

## 2  Related Works

Image authentication techniques include image forgery detection, manipulation detection, digital signatures, and perceptual hashing. In image forgery detection, the image is processed using two methods: active and passive [4,5]. The active detection refers to the insertion of additional information incorporated into an image before transmission, such as digital watermarking [6]; whereas the passive detection utilizes statistical approaches to locate the feature's changes in an image [7]. Many passive techniques for detecting image splicing have been presented throughout the years (discussed below, and a summary of recent studies is presented in Table 1). The detection of image splicing forgeries is based on the details that remain after the modification. Inconsistency, edge discontinuity, and geometric and illumination circumstances are some of the most typical image splicing concerns. Forgery detection was accomplished using a statistical model based on discrete wavelet transforms (DWT) and discrete cosine transforms (DCT). These approaches are based on detecting forgeries within images by identifying the statistical dependency among image pixels [8,9].

In Parnak et al. [10] a forgery detection system based on Benford's law variants and another statistical feature extraction was proposed. SVM was used as the main classifier, and the method was tested on two popular image datasets. In this algorithm, the RGB input is transformed into YCbCr, and

after image blocking, two-dimensional DCT is applied to each block. Despite the shown high detection accuracy, this approach has low precision in some circumstances, such as small forged sections. It is reported that Jaiprakash et al. [11] used the statistics and correlation found by DWT and DCT to detect image forgeries. This approach achieved 89.5% accuracy with a 212-D feature vector. However, the approach demonstrated a difficulty in identifying the traces detected in the forged images.

Using a similar approach, Li et al. [12] applied SVM to detect image splicing using a Markov feature vector in a quaternion DCT. With a feature dimension of 972, their technique produced an accuracy rate of 92.38%. However, the limitation of the Markov component in the quaternion DCT model increased the complexity and time consumption of the splicing approach.

For forged image detection involving conformable focus measures model for feature extraction, Subramaniam et al. [13] proposed a combination of feature extractions in "redundant discrete wavelet transforms (RDWT)" to enhance the image forgery detection. By combining conformable focus measurements and focus measure operators, the study enhanced the splicing detection accuracy up to 98.6% with 24 extracted feature vectors. However, their proposed method is time consuming due to multiple approaches to feature extraction.

**Table 1:** Summary of recent studies which deal with the image forgery

| References | Method | Accuracy | Limitations |
|---|---|---|---|
| Al-Azawi et al. [4] | Four rounds of feature extraction to obtain essential elements from suspicious images: local binary patterns (LBP), Fractal Entropy (FrEp), Kurtosis and Skewness. | 98% | This approach has an enormous number of features and thus high computational complexity. |
| El-Latif et al. [7] | A deep learning-based approach with feature dimension of 1024 for detecting forged images. | 96% | This method has a large number of features and a high level of computational complexity. |
| Parnak et al. [10] | A forgery detection system based on Benford's law variants. | 99% | This approach has low precision in some circumstances, such as small, forged sections. |
| Jaiprakash et al. [11] | Feature extraction using DWT and DCT to detect image forgeries. | 89.5% | This approach demonstrated a difficulty in identifying the forged traces in the forged images. |
| Li et al. [12] | Apply the SVM to detect image splicing using a Markov feature vector in a quaternion DCT. | 92.38% | This approach has a time consuming splicing approach. |
| Jalab et al. [14] | A combination of feature extractions in "redundant discrete wavelet transforms (RDWT)" to enhance the forgery detection. | 98.6% | Multi approaches to feature extraction require significantly more time and computational resources. |
| Rao et al. [15] | Two sets of texturing algorithms are applied in conjunction with the SVM. | 97% | The model's overall performance has a high computational cost. |
| Souradip et al. [16] | This method utilized local feature descriptors from either RGB color or grayscale images learned by two-branch CNN with SVM. | 97% | This method has a high computational complexity cost. |
| Doegar et al. [17] | A blind image detection approach using a deep residual CNN network, followed by a classifier network. | 96% | The complexity of feature extraction in this approach is high. |
| Whittaker [18] | A transfer learning-based approach that uses the AlexNet model's pre-trained weights to reduce the training time. | 93% | The model has a high computational cost. |

Another approach for image splicing detection was proposed by [14] to enhance images for better detection of image splicing. To identify the important features from spliced images, two sets of texturing algorithms are applied in conjunction with the SVM classifier to differentiate between authentic and spliced images. The suggested model achieved an accuracy rate of 97%. This approach used an image enhancement model prior to image forgery detection. However, the usage of image enhancement as a preprocessing step prior to feature extraction suggests that the features' quality was inefficient.

Unlike the above-mentioned model-based approaches, which require creating handcrafted features, the deep learning-based methodologies can directly learn and categorize features for image forgery detection. A deep learning approach was proposed for image forensics by Rao et al. [15]. This method utilized local feature descriptors from either RGB color or grayscale images learned by two-branch convolutional neural network (CNN) with SVM classifier for image splicing detection. Applying normal CNN architecture to image forensic tasks results in a rather low performance and high complexity of computation cost. El-Latif et al. [7] developed a deep learning-based approach with feature dimension of 1024 for detecting forgery images. The approach was tested using two publicly available image splicing datasets. SVM classifier is used to classify the final features. The primary limitations are the enormous number of features and the high complexity of computations. Souradip et al. [16] developed a blind image detection approach using a deep residual CNN network, followed by a classifier network. The achieved accuracy was 96% on CASIA v2.0 dataset. However, this detection technique has certain limitations in terms of feature extraction complexity. In another study, Doegar et al. [17] presented a transfer learning-based approach that uses the AlexNet model's pre-trained weights to reduce the training time. SVM is used as a classifier in this strategy. The model's overall performance was decent in terms of accuracy and computational resources.

Despite great accuracy, deep learning necessitates a big image dataset with hardware support. This can be seen as a drawback when attempting to create an effective algorithm. In this study, we propose a novel method for detecting forgery images based on Whittaker function as texture feature extraction model. To do this, the input RGB image is converted to a YCbCr image, and following image blocking, each block is subjected to a two-dimensional DWT. Following that, features based on Whittaker function are extracted to create a final feature vector. Finally, for classification, SVM is used.

The proposed method in this study utilizes the image dataset CASIA V2.0. The methodology is simple to implement, and the proposed Whittaker function technique may extract powerful features from images, allowing an SVM to perform classification efficiently and quickly. The main contribution of this study is the novel Whittaker function-based image feature extraction model (GKSWF) for a better and more efficient image forgery detection.

## 3 Proposed Model

The primary goal of this study is to improve image forgery detection by using a generalized k-symbol Whittaker function (GKSWF) as a texture feature extraction model. Fig. 3 illustrates the steps of the proposed image authentication model, which includes pre-processing, feature extraction using GKSWF, dimensionality reduction, and finally classification.
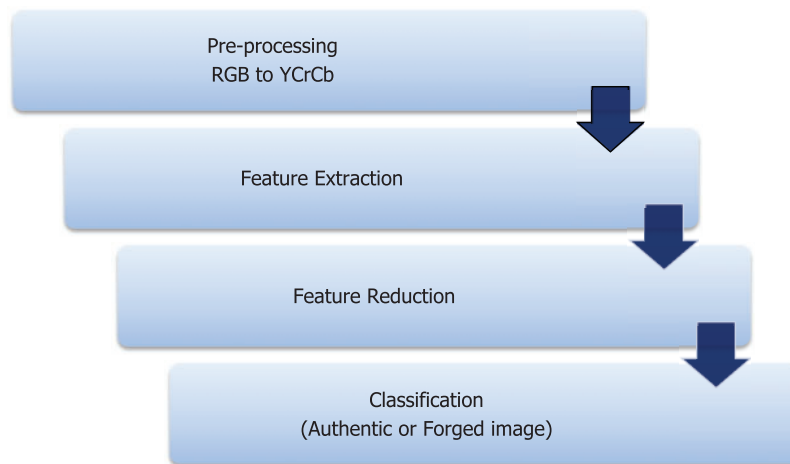
**Figure 3:** Block diagram of the proposed image authentication model

### 3.1 Preprocessing

Pre-processing step is used to obtain a better feature extraction, which would improve the algorithm's accuracy later. The color input image is transformed in the YCbCr color space. The RGB color space is the most common and frequently utilized in digital imaging. While RGB has advantages compared with other color spaces, it is unsuitable for use in forgery detection due to the relation of red, green, and blue which is particularly strong. The advantages of using the YCbCr in image splicing detection are described in [14]. Fig. 4 illustrates an RGB image and its YCbCr version, complete with channels. The image is divided into numerous non-overlapping blocks of size 8 × 8 in the pre-processing step, and then the texture features are calculated.
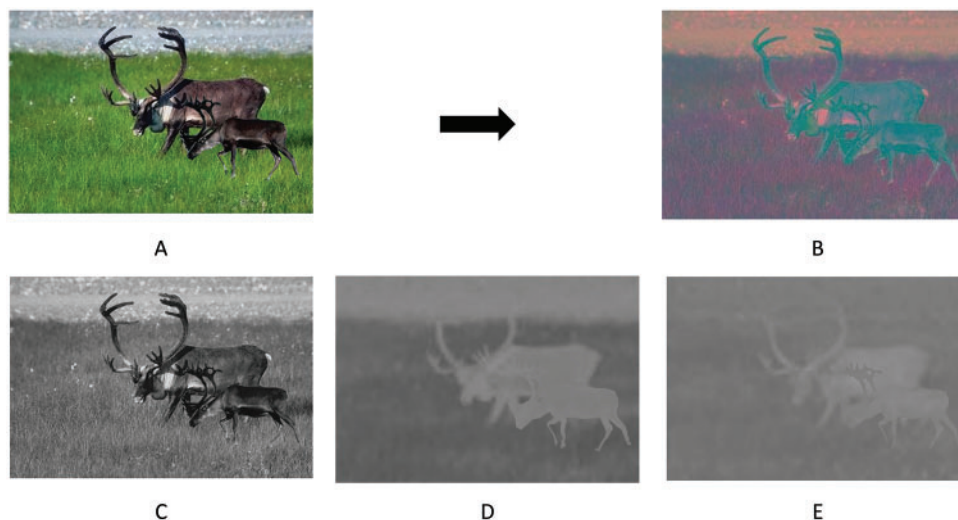


**Figure 4:** Pre-processing of a sample RGB image. (A) is RGB color space, (B) is YCbCr color space, (C) is Y color space, (D) is Cb color space, (E ) is Cr color space

### 3.2 Proposed Feature Extraction Algorithm

Whittaker (1903) created a modified version of the confluent hypergeometric equation, known as Whittaker's equation. Whittaker's equation is given in the form [18]:

$$\frac{d^2\omega}{d\chi^2} + \left(-\frac{1}{4} + \frac{\alpha}{\chi} + \frac{1/4 - \beta^2}{\chi^2}\right)\omega = 0, \tag{1}$$

where the first solution is

$$\omega_{\alpha,\beta} = exp\left(-\chi/2\right)\chi^{\beta+1/2}\sum_{n=0}^{\infty}\left(\frac{(\beta - \alpha + 1/2)_n}{n!\,(2\beta + 1)_n}\right)\chi^n = exp\left(-\chi/2\right)\chi^{\beta+1/2}\sum_{n=0}^{\infty}\left(\frac{(\beta - \alpha + 1/2)_n}{\Gamma\,(n+1)\,(2\beta + 1)_n}\right)\chi^n$$

$$= exp\left(-\chi/2\right)\chi^{\beta+1/2}\left(1 + \frac{1/2 + \beta - \alpha}{1!\,(2\beta + 1)}\chi + \frac{(1/2 + \beta - \alpha)\,(3/2 + \beta - \alpha)}{2!\,(2\beta + 1)\,(2\beta + 2)}\chi^2 + \ldots\right)$$

$$= exp\left(-\chi/2\right)\chi^{\beta+1/2}\left(1 + \frac{1/2 + \beta - \alpha}{\Gamma\,(2)\,(2\beta + 1)}\chi + \frac{(1/2 + \beta - \alpha)\,(3/2 + \beta - \alpha)}{\Gamma\,(3)\,(2\beta + 1)\,(2\beta + 2)}\chi^2 + \ldots\right)$$

$$\tag{2}$$

The second solution is $\omega_{\alpha,-\beta}$, where $(P)_n$ indicates the Pochhammer symbol.

This concept of k-symbol is formulated by Diaz and Osler [19,20], as follows:

**Definition 1**

The motivate gamma function, sometimes known as the k-symbol gamma function, is assumed by the formula:

$$\Gamma_k\left(\Upsilon\right) = lim_{n\to\infty}\frac{n!\,k^n(nk)^{\frac{\Upsilon}{k}-1}}{(\Upsilon)_{n,k}}, \tag{3}$$

where

$$(\Upsilon)_{n,k} := \Upsilon(\Upsilon + k)(\Upsilon + 2k)\ldots(\Upsilon + (n-1)k)$$

and

$$(\Upsilon)_{n,k} = \frac{\Gamma_k(\Upsilon + nk)}{\Gamma_k(\Upsilon)}. \tag{4}$$

Note that $\Gamma_k(\Upsilon) \to \Gamma(\Upsilon)$ when $k \to 1$, and $\Gamma_k(\Upsilon + k) = \Upsilon\Gamma_k(\Upsilon)$, $\Gamma_k(k) = 1$.

Based on the k-symbol definition, k-symbol Whittaker's function can be generalized as follows:

$$T = exp(-\chi/2)\chi^{\beta+1/2}\sum_{n=0}^{\infty}\left(\frac{(\beta - \alpha + 1/2)_{n,k}}{\Gamma_k(n+1)(2\beta + 1)_{n,k}}\right)\chi^n \tag{5}$$

Note that when $k = 1$, the classic Whittaker's function is obtained. The fractional parameters $\langle,\beta$ are experimentally fixed to 0.5, and $k$ is the k-symbol $\epsilon$ N, while $\chi^n$ is the image's pixel probability. As a feature extraction model, the proposed GKSWF is intended to extract texture details of tampered information based on image pixel probability, which is the main contribution of this study.

The proposed GKSWF-based model is done through the following steps:

1. Read the input image.
2. Experimentally fix the fractional parameters $\alpha$, $\beta$ and the k-symbol.
3. Convert the original image's color space from RGB to YCbCr.
4. Divide each color space image into $8 \times 8$ pixel blocks, which are set experimentally.

5. Determine the texture feature (T) for each image block using Eq. (5).
6. Feature dimensionality reduction using Mean, Variance, Skewness, and Kurtosis. The final 12 features make up the final feature vector.
7. As the final texture feature, save the texture feature vector for all image blocks.
8. The SVM classifier is utilized to categorize images into two groups: authenticate or spliced images.

The image collection is divided into training and testing steps for SVM classification.

    A: Training procedures.
(1) Read all training images from the training image set and extract features using steps 1–7.
(2) Assign a value of 0 to the authentic images and a value of 1 to the spliced images in the training features.

    B: Testing Procedures
(1) Read an image from the testing image set and extract features using steps 1–7.
(2) Put the feature to the test with the corresponding trained SVM.
(3) Repeat steps 1–3 until all images are tested.

As previously stated, the image forgery has a direct impact on textural aspects. The distribution of textural qualities gives a quantitative basis for distinguishing authentic from forged images. Fig. 5 depicts this behavior using a scatter plot. This plot demonstrates that the two classes (i.e., authentic and forged) are distinct.
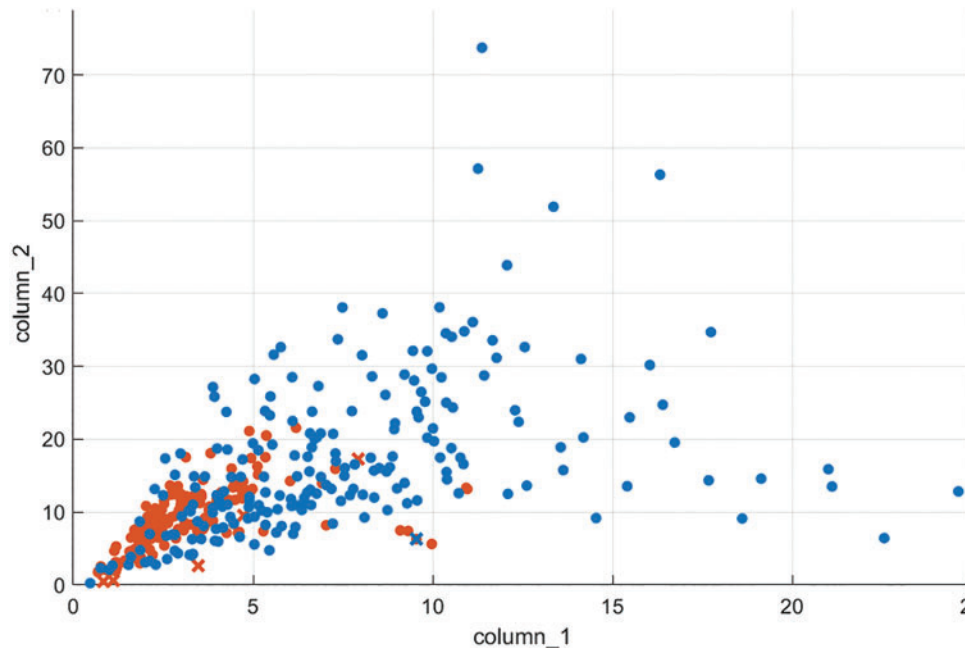


**Figure 5:** The distribution of authentic (red dots) and forged (blue dots) features

The dimensionality reduction of features are applied in order to reduce computational cost and resource allocation. This ensures the algorithm is working at its most efficient and optimal settings. The "Mean", "Variance", "Skewness", and "Kurtosis" are employed in the current work to reduce the dimensionality of the extracted data in each image by the proposed feature extraction model.

For features F of M scalar observations, the "Mean" is defined as

$$Mn = \frac{1}{M} \sum_{I=1}^{M} F_i \tag{6}$$

The "Variance" is defined as

$$Vc = \frac{1}{M-1} \sum_{i=1}^{NM} |F_i - \mu|^2 \tag{7}$$

where μ is the "Mean" of $F_i$

The 'Skewness' is a quantity of the asymmetry of the feature data around the feature mean, and is defined as

$$Ss = \frac{V(x-\mu)^3}{\sigma^3} \tag{8}$$

where $\sigma$ is the 'Standard deviation', and V(t) denotes the estimated value of the quantity t.

The 'Kurtosis' is defined as

$$Ks = \frac{V(x-\mu)^4}{\sigma^4} \tag{9}$$

The 'Standard deviation' is defined as

$$St = \sqrt{\frac{1}{M-1} \sum_{i=1}^{M} |F_i - \mu|^2} \tag{10}$$

### 3.3 The Classification

The SVM classifier, which is utilized in a variety of applications, was used in this study using the MATLAB R2021b [21].

### 3.4 Evaluation Metrics

The following metrics are utilized for evaluating the performance of the proposed model.

$$TPR = \frac{TP}{TP + FN} \tag{11}$$

$$TNR = \frac{TN}{TN + FP} \tag{12}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \tag{13}$$

where TP ("True Positive") and TN ("True Negative") specify the number of forged and authentic images that have been correctly classified, whereas FN ("False Negative") and FP ("False Positive") are the number of forged and authentic images that are incorrectly labeled.

## 4 Experimental Results and Discussion

All the tests were executed using MATLAB 2021b. The 5-fold cross-validation is applied in this study. The dataset is partitioned into five subsets, and the main procedure is repeated five times, with 70% of the images used for training and 30% used for testing in each iteration.

In this study, a publicly available "CASIA V2.0" dataset is used [22]. The dataset contains 12614 images, 7491 (60%) of which are authentic and 5123 (40%) are forged. This dataset has undergone many transformation procedures as well as some post-processing, resulting in a complete dataset.

Furthermore, this dataset has been utilized in the literature and is considered as a standard in the field of image splicing detection. Fig. 6 shows examples of CASIA v2 image dataset.



**Figure 6:** CASIA V2.0 dataset samples, the first and second rows have authentic images, whereas the third row has spliced images

The feature extraction procedure begins by dividing the image into non-overlapping blocks, then extracting the texture features from each block. To evaluate the effect of image block size on the detection process, the non-overlapping blocks were set to the size (8 × 8, 16 × 16, 32 × 32, 64 × 64, and 128 × 128) pixels. The best detection accuracy results were achieved with an image block size of 8 × 8 pixels. The findings in Fig. 7 show that the proposed technique can achieve accuracy rates of 98.60% with 12-D features. The "reception operating characteristic" (ROC) curve and associated score "area under the curve" (AUC) are other methods for validating classification findings. By graphing the TP and FP rates, this curve depicts categorization performance at all thresholds. Fig. 8 illustrates the proposed model's ROC curve. The AUC is equal to 0.98 (higher is better), indicating that the categorization classes are better separated.

The experimental findings in Table 2 demonstrates that the proposed method achieved the best forgery detection results. This shows how effective the method is at detecting authentic or forged images. The study in [14] slightly outperforms our method in terms of forgery detection accuracy by 0.40%, owing to the use of multiple feature extraction algorithms, which improved classification accuracy but was computationally more intensive. Moreover, the study [15] among other approaches, achieved the second greatest accuracy, this is because, this study used an image enhancement method before feature extraction and classification which enhanced the classification accuracy. It is also worth noting that deep learning CNN-based methods [7,17,23] have been used to detect forgery images. The study in [23] achieved the second-best detection accuracy of 97.24%. This leads to the conclusion that the deep learning CNN-based method exhibits good robustness with high complexity. On the contrary, the proposed method achieves the acceptable detection accuracy while using the fewest

feature dimensions. This demonstrates the method's usefulness and reliability, as well as the value of employing the k-Symbol Whittaker function as a texture descriptor.
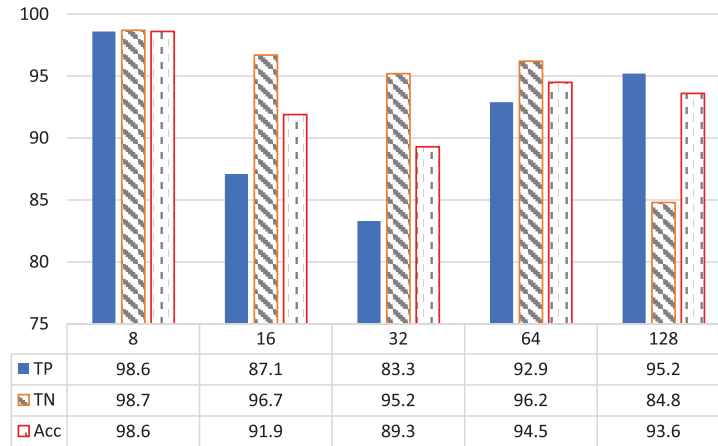


| | 8 | 16 | 32 | 64 | 128 |
|---|---|---|---|---|---|
| TP | 98.6 | 87.1 | 83.3 | 92.9 | 95.2 |
| TN | 98.7 | 96.7 | 95.2 | 96.2 | 84.8 |
| Acc | 98.6 | 91.9 | 89.3 | 94.5 | 93.6 |

**Figure 7:** Detection accuracy of the proposed feature extraction method in different image block dimensions
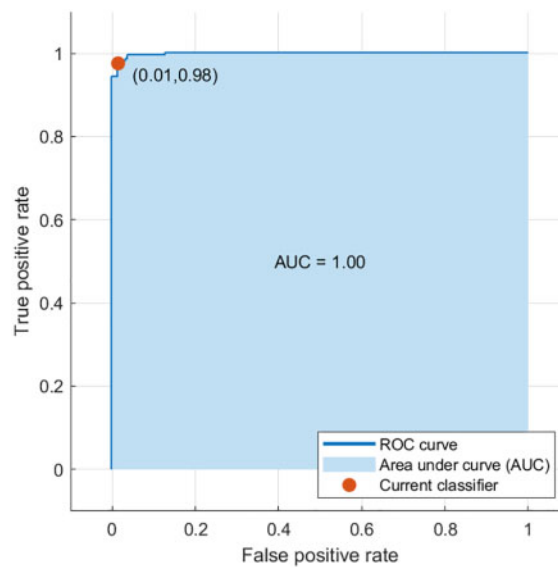


**Figure 8:** ROC for the proposed model

**Table 2:** The comparison results on CASIA 2.0 dataset

| Methods | Features dimensions | TPR (%) | TNR (%) | Accuracy (%) |
|---|---|---|---|---|
| Al-Azawi et al. [4] | 4 | 97 | 96 | 98 |
| Jaiprakash et al. [11] Cr | 212 | 89.10 | 90.90 | 89.50 |
| Li et al. [12] | 972 | 49.00 | 93.00 | 92.38 |
| El-Latif et al. [7] | 1024 | 96.00 | 96.45 | 96.36 |

(Continued)

**Table 2:** Continued

| Methods | Features dimensions | TPR (%) | TNR (%) | Accuracy (%) |
|---|---|---|---|---|
| Subramaniam et al. [13] Cb and Cr | 48 | 99 | 96 | 97.90 |
| Jalab et al. [14] Cb | 28 | 98.80 | 98.00 | 98.40 |
| Souradip et al. [16] | – | 96.69 | 94.15 | 96.45 |
| Meena et al. [23] | – | – | – | 97.24 |
| Proposed Method Y, Cb, and Cr | 12 | 98.60 | 98.70 | 98.60 |

## 5 Conclusion

A novel texture descriptor algorithm based on generalized k-symbol Whittaker function (GKSWF) for better splicing detection has been proposed. The proposed GKSWF intends to preserve image information in the smooth regions, while extracting clues of tampering texture details. When tested on the CASIA V2.0 dataset, the proposed method achieved an accuracy rate of 98.60% with a feature size of 12. The proposed method is superior to similar methods due to its excellent classification accuracy with the least feature dimension. The study's limitation is that it cannot determine where the images have been tampered with. Future research could try to use the current method to detect and locate the tampered region within the forged images.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1]  X. Zhao, P. Bateman and A. T. Ho, "Image authentication using active watermarking and passive forensics techniques," in *Multimedia Analysis, Processing and Communications*, Berlin: Springer, vol. 2011, pp. 139–183, 2011.

[2]  F. Wang, W. L. Lyu and J. S. Pan, "Robust image authentication scheme with self-repair capability for greyscale source document images via PNG format," *IET Image Processing*, vol. 10, no. 12, pp. 971–978, 2016.

[3]  R. W. Ibrahim, Z. Moghaddasi, H. A. Jalab and R. M. Noor, "Fractional differential texture descriptors based on the Machado entropy for image splicing detection," *Entropy*, vol. 17, no. 7, pp. 4775–4785, 2015.

[4]  R. J. Al-Azawi, N. M. Al-Saidi, H. A. Jalab, R. W. Ibrahim and D. Baleanu, "Image splicing detection based on texture features with fractal entropy," *CMC-Computers Materials & Continua*, vol. 69, no. 3, pp. 3903–3915, 2021.

[5]  S. Sadeghi, S. Dadkhah, H. A. Jalab, G. Mazzola and D. Uliyan, "State of the art in passive digital image forgery detection: Copy-move image forgery," *Pattern Analysis and Applications*, vol. 21, no. 2, pp. 291–306, 2018.

[6]  A. N. Yahya, H. A. Jalab, A. Wahid and R. M. Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network," *Journal of King SAUD UNIVERSITY-Computer and Information Sciences*, vol. 27, no. 4, pp. 393–401, 2015.

[7]   A. El-Latif, I. Eman, A. Taha and H. H. Zayed, "Passive approach for detecting image splicing using deep learning and Haar wavelet transform," *International Journal of Computer Network & Information Security*, vol. 11, no. 5, pp. 1–15, 2019.

[8]   L. Leng, M. Li, C. Kim and X. Bi, "Dual-source discrimination power analysis for multi-instance contactless palmprint recognition," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 333–354, 2017.

[9]   L. Leng, J. Zhang and K. Alghathbar, "Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain," *International Journal of Physical Sciences*, vol. 5, no. 17, pp. 2543–2554, 2010.

[10]  A. Parnak, Y. Damavandi and S. Kazemitabar, "Novel image splicing detection algorithm based on generalized and traditional benford's law," *International Journal of Engineering*, vol. 35, no. 4, pp. 626–634, 2022.

[11]  S. P. Jaiprakash, M. B. Desai, C. S. Prakash, V. H. Mistry and K. L. Radadiya, "Low dimensional DCT and DWT feature based model for detection of image splicing and copy-move forgery," *Multimedia Tools and Applications*, vol. 79, no. 39, pp. 29977–30005, 2020.

[12]  C. Li, Q. Ma, L. Xiao, M. Li and A. Zhang, "Image splicing detection based on Markov features in QDCT domain," *Neurocomputing*, vol. 228, no. 3, pp. 29–36, 2017.

[13]  T. Subramaniam, H. A. Jalab, R. W. Ibrahim and N. F. M. Noor, "Improved image splicing forgery detection by combination of conformable focus measures and focus measure operators applied on obtained redundant discrete wavelet transform coefficients," *Symmetry*, vol. 11, no. 11, pp. 1392–1404, 2019.

[14]  H. A. Jalab, M. A. Alqarni, R. W. Ibrahim and A. A. Almazroi, "A novel pixel's fractional mean-based image enhancement algorithm for better image splicing detection," *Journal of King Saud University-Science*, vol. 34, no. 2, pp. 1–15, 2022.

[15]  Y. Rao, J. Ni and H. Zhao, "Deep learning local descriptor for image splicing detection and localization," *IEEE Access*, vol. 8, no. 4, pp. 25611–25625, 2020.

[16]  N. Souradip and R. Naskar, "Automated image splicing detection using deep CNN-learned features and ANN-based classifier," *Signal, Image and Video Processing*, vol. 2021, no. 15, pp. 1601–1608, 2021.

[17]  A. Doegar and K. Gaurav, "CNN based image forgery detection using pre-trained alexnet model," *International Journal of Computational Intelligence & IoT*, vol. 2, no. 1, pp. 402–407, 2019.

[18]  J. M. Whittaker, "On the cardinal function of interpolation theory," *Proceedings of the Edinburgh Mathematical Society*, vol. 1, no. 1, pp. 41–46, 1927.

[19]  J. Diaz and T. Osler, "Differences of fractional order," *Mathematics of Computation*, vol. 28, no. 125, pp. 185–202, 1974.

[20]  R. Diaz and E. Pariguan, "On hypergeometric functions and Pochhammer k-symbol," *arXiv preprint math*, vol. 45, no. 596, pp. 1–14, 2004.

[21]  *Matlab tools. The Mathworks Inc, Natick, Massachusetts,USA. 2021,* https://www.mathworks.com

[22]  *CASIA Tampered image detection evaluation database (CASIA TIDE v2.0). [Online]. Accessed on July 2022. Available:* http://forensics.idealtest.org:8080/index_v2.html

[23]  K. Meena and V. Tyagi, "A deep learning based method for image splicing detection," *Journal of Physics: Conference Serie*, vol. 2021, no. 1, pp. 1–12, 2021.