University of Baghdad
College of Engineering
JE
JOURNAL OF ENGINEERING

Journal of Engineering

journal homepage: www.jcoeng.edu.iq

Volume 30 Number 6 June 2024

Copy Move Image Forgery Detection using Multi-Level Local Binary Pattern Algorithm

Marwa Emad Mahdi [1,*], Nada Hussein M Ali [2]

Department of Computer, College of Sciences, University of Baghdad, Baghdad, Iraq
marwa.Emad1201a@sc.uobaghdad.edu.iq[1], nada.husn@sc.uobaghdad.edu.iq[2]

ABSTRACT

Digital image manipulation has become increasingly prevalent due to the widespread availability of sophisticated image editing tools. In copy-move forgery, a portion of an image is copied and pasted into another area within the same image. The proposed methodology begins with extracting the image's Local Binary Pattern (LBP) algorithm features. Two main statistical functions, Stander Deviation (STD) and Angler Second Moment (ASM), are computed for each LBP feature, capturing additional statistical information about the local textures. Next, a multi-level LBP feature selection is applied to select the most relevant features. This process involves performing LBP computation at multiple scales or levels, capturing textures at different resolutions. By considering features from multiple levels, the detection algorithm can better capture both global and local characteristics of the manipulated regions, enhancing the accuracy of forgery detection. To achieve a high accuracy rate, this paper presents a variety of scenarios based on a machine-learning approach. In Copy-Move detection, artifacts and their properties are used as image features and support Vector Machine (SVM) to determine whether an image is tampered with. The dataset is manipulated to train and test each classifier; the target is to learn the discriminative patterns that detect instances of copy-move forgery. Media Integration and Call Center Forgery (MICC-F2000) were utilized in this paper. Experimental evaluations demonstrate the effectiveness of the proposed methodology in detecting copy-move. The implementation phases in the proposed work have produced encouraging outcomes. In the case of the best-implemented scenario involving multiple trials, the detection stage achieved a copy-move accuracy of 97.8 %.

Keywords: Support vector machine, Copy-Move, MICC-F2000, Local binary pattern, Multi Local binary pattern.

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2024.06.09

Article received: 07/07/2023
Article accepted: 25/09/2023
Article published: 01/06/2024

كشف تزوير نسخ الصور باستخدام خوارزمية النمط الثنائي المحلي متعدد المستويات

مروه عماد مهدي[1] ,ندى حسين محمد علي [2]

قسم الحاسوب، كلية العلوم, جامعة بغداد، بغداد،العراق

الخلاصة

أصبح التلاعب بالصور الرقمية سائدًا بشكل متزايد بسبب التوافر الواسع لأدوات تحرير الصور المتطورة. في تزييف نقل النسخ ، يتم نسخ جزء من الصورة ولصقه في منطقة أخرى داخل نفس الصورة. تبدأ المنهجية المقترحة باستخراج ميزات خوارزمية *LBP* للنمط الثنائي المحلي من الصورة. يتم حساب وظيفتين إحصائيتين رئيسيتين *STD* و *ASM* لكل ميزة *LBP* ، مع التقاط معلومات إحصائية إضافية حول القوام المحلي. بعد ذلك ، يتم تطبيق تحديد ميزة *LBP* متعدد المستويات لتحديد الميزات الأكثر صلة. تتضمن هذه العملية إجراء حساب *LBP* على مستويات أو مستويات متعددة ، والتقاط مواد بدقة مختلفة. من خلال النظر في الميزات من مستويات متعددة ، يمكن لخوارزمية الاكتشاف أن تلتقط بشكل أفضل الخصائص العالمية والمحلية للمناطق التي تم التلاعب بها ، مما يعزز دقة اكتشاف التزوير. لتحقيق معدل عالٍ من الدقة ، تم توظيفهم في مجموعة متنوعة من السيناريوهات بناءً على نهج التعلم الآلي. في اكتشاف *Copy–Move* ، تُستخدم القطع الأثرية وخصائصها كميزات للصورة ، و *Support Vector Machine (SVM)* لتحديد ما إذا كان قد تم العبث بالصورة أم لا. يتم التلاعب بمجموعة البيانات لتدريب واختبار كل مصنف ، والهدف هو معرفة الأنماط التمييزية التي تميز المناطق التي تم التلاعب بها عن تلك الأصلية ، وبالتالي اكتشاف حالات تزوير نقل النسخ.تم استخدام تكامل الوسائط وتزوير مركز الاتصال (*MICC–F2000*) في هذه الورقة ، حيث توضح التقييمات التجريبية فعالية المنهجية المقترحة في اكتشاف نقل النسخ. أسفرت مراحل التنفيذ في العمل المقترح عن نتائج مشجعة. في حالة أفضل سيناريو تم تنفيذه والذي يتضمن تجارب متعددة ، حققت مرحلة الاكتشاف دقة نقل نسخ تبلغ % 97.8.

الكلمات المفتاحية: دعم آلة المتجهات، نقل النسخ، MICC–F2000 ، النمط الثنائي المحلي ، النمط الثنائي المحلي المتعدد.

1. INTRODUCTION

The popularity of image editing software has made it increasingly easy to alter the content of images **(Agarwal and Mane, 2016).** These alterations threaten the authenticity and integrity of images, causing misjudgments and possibly even affecting social stability **(Al-Bayati et al., 2020).** The digital image remains an important component of information expansion in traditional **(Wang, 2017)** regular communication, such as social networks, websites, newspapers, television, and journals **(Asghar et al., 2017)**. There is a big risk of alteration and integrity attacks owing to the saturation of the digital image broadcast on a routine basis on mobile **(Salih et al., 2023)** and the simple-to-arrival multimedia channel (e.g., net) **(Abidin et al., 2019)**. Furthermore, the easy availability of low-cost and efficient images of code-editing content (such as Adobe Photoshop and Pixar) **(Prinkle and Jyoti, 2015)** has cast doubt on the validity and safety of images **(Anbu et al., 2017)**. False, frequently edited photographs have become a worldwide scourge, especially with the widespread use of social media as a modern substitute for traditional news outlets. **(Wu et**

al., 2018). This phenomenon can be broadly referred to the two points:(1) the fast-dropping price of digital cameras and phones, which brings an increase in the digital image, and (2) the availability and simple of- utilize of images-rewriting software (such as Mobile apps, open sources materials) that render it profoundly simple to edit or manipulate pictures, either for innocuous or malicious intent **(Abdalla et al., 2020)**. The software package allows users to create special effects indistinguishable from genuine photos or obtain hybrid-generated visual content **(Al-Qershi and Khoo, 2013)** Nowadays, digital photos have been used not only as master loads of information but also as a sort of certificate for a criminal court. Aside from that, maintaining correctness and safety in digital images has been a major concern in recent years **(Dhivya et al., 2020; Hassan and Moayed, 2023)**.

Several strategies have been proposed to detect various types of image manipulation copy transmission of fake images. These works aim to achieve authentication of the image to avoid forgery. **(Chang et al., 2013)** applied the Local Binary Pattern (LBP) function to each block in the image to produce the authentication **(Hassoon and Jalil, 2022)**. The current image block's pixel was indicated according to the block mapping sequence, and then LBP was inserted into the 2- LSBs of the related image block. Finally, the identification and recovery of image tampering are performed. The eight binary mean values optimize the recovery for every eight neighboring pixels in the image, where the tamper detection rate of the proposed scheme is over 95%**.**

(Manu and Mehtre, 2016) suggested a CMFD strategy based on DCT and ORB feature extraction and a distance-based clustering approach **(Ibrahim et al., 2020).** The extracted DCT features are compared using Euclidean distance. Key points extracted with ORB are matched using the k-NN process based on Hamming distances. The proposed method is used. The accuracy of the results was approximately 96%. **(Zhang et al., 2018)** provided an approach to increase the detection efficiency of the DWT-based technology (**AL Shibani and Sadeq, 2018)**. Originally, the DWT block was applied to the input images, and Markov features were created to explain the dependence of wavelet coefficients across positions. Lastly, SVM was used to differentiate between real and spliced photos **(Abdul-Samad and Kamal., 2020)**. Tests revealed that the detection efficiency of the features acquired in DWT was 89% in the optimal combination of block size and feature number. The study of **(Dhivya et al., 2020)** applied Speeded Up Robust Feature (SURF) feature extraction, and the specific item was detected using a support vector machine. The image was altered several times during the copy-move ruse **(Babu and Rao, 2022)**. The image rotation function, which contains bicubic and crop operations, is used by the feature-matching method in this example and extracted features from a set of test images **(Hamid and Jamel, 2022).** The results of the tests suggest that the proposed technique can yield significant and stunning results**. (Solaiyappan and Wen, 2022)** seek to address the detection of such attacks through a structured case study. They test eight machine learning algorithms, including three traditional machine learning approaches (Support Vector Machine, Random Forest, and Decision Tree) **(Huang et al., 2018)**, in differentiating between tampered and untampered photos. The models extract features, and each pre-trained model is fine-tuned **(Suresh and Rao, 2016).** This study's findings indicate near-perfect accuracy in detecting tum, injections, and removals.

The proposed system aims to detect and classify digital image forgeries by implementing a dedicated forgery detection mechanism. The proposed system employs a set of statistical functions to ensure high accuracy in the classification process. This research focuses on developing an effective technique for extracting features from digital images, enabling the

utilization of these feature vectors in various image processing applications, such as forgery identification. The method used to classify images as authentic or tampered relies on hand-crafted features and an SVM classifier.

2. IMAGE FORGERY TYPES

Two approaches are used for image forgery detection: active and passive, the image forgery classification techniques are shown in **Fig.1.**

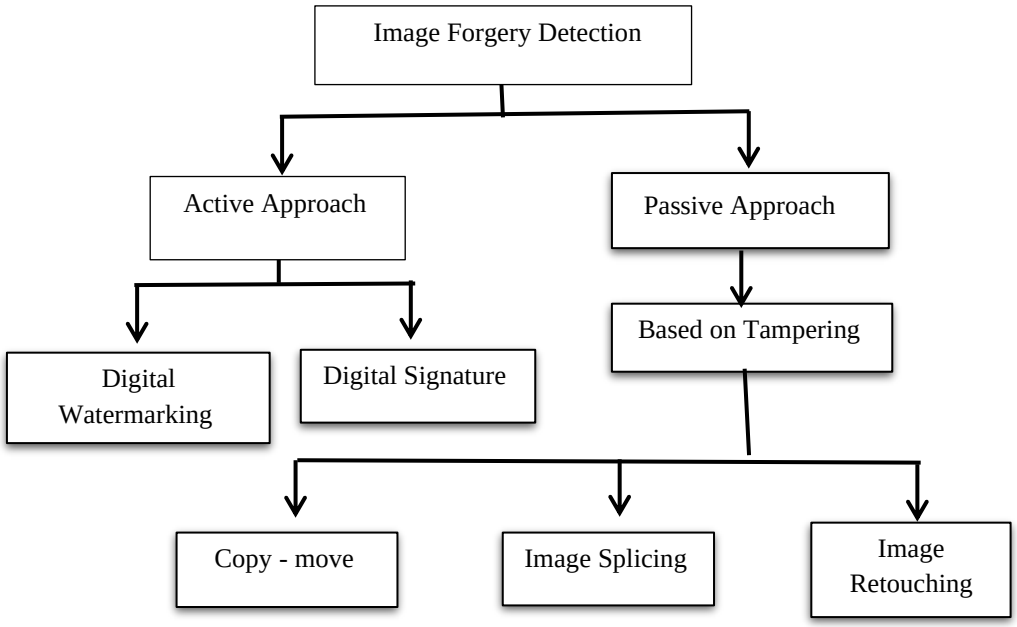

Figure 1. Image forgery classification techniques **(Thakur et al., 2018)**

The first type is image tampering, which is one of the most widely employed to hide or add new information to an image by copying a portion of the image and pasting one or more copies of it on the same image **(Lin et al., 2017),** a technique known as a copy-move forging (**Kaur, 2016**), as illustrated in **Fig. 2**.

(a) Original image (b) Copy-move image

Figure 2. Copy-Move Forgery **(Dhir, 2017)**

The second sort of forgery is splicing image forgery, which is the most aggressive type; it is accomplished by clipping a portion of a picture and splicing (pasting) it onto another image **(Jaiswal and Srivastava, 2020).** When such splicing is done carefully, the boundaries between the splicing regions are undetected, making tampering perilous **(Dhivya et al., 2020)**. **Fig. 3** depicts a splicing forgery example where images labeled (a) and (b) are original images and the image with the label (c) is a splicing image.

(c) Splicing image

Figure 3. Image Splicing Forgery **(Kumar and Srivastava, 2017)**

The third image forgery is the least disruptive, in which the original image does not change significantly, but specific parts are improved or optimized **(Abdul Hossen et al., 2022)**. The first category is picture editing **(Akram et al., 2022)**, used in publications to improve an image's quality and make it more appealing. Such methods are primarily used in smartphone camera filters **(Kumar and Srivastava, 2017). Fig. 4** depicts this form of picture fabrication

(a) Original image (b)Retouched image

Figure 4. Image retouching forgery **(Dhir, 2017)**

2. Copy-Move Forgery Detection Methodology

The proposed image tampering detection consists of five main phases: reading dataset, Pre-processing, feature extraction, and selection, training, and testing, as well as classification each phase contains some stages, will be implemented and each stage will be described briefly.

2.1 MICC-F2000 Datasets

The MICC-F2000 dataset is well-known for testing and comparing the performance of various forgery detection systems. These forgeries photos in these datasets are made by cloning bits of the original image and pasting them into the same image to question the image's legitimacy. Fake photos have been subjected to transformations such as rotation (90, 180-degree angle), transition, scaling, or a combination. These datasets are made up of photos of various sizes. The image examples are drawn from the tampered-with and original MICC-F2000 data set. The MICC-F2000 data collection comprises images of various sizes, and it is in JPEG image format. The MICC is part of Florence University's Knowledge Engineering Division. It is a multidisciplinary research institution focused on video and image processing, transmission, and interpretation, as well as synthetic vision and multimedia approaches applied to health, social applications, and cultural heritage. The graphic depicts several dataset samples from the MICC-F2000 dataset that have been tampered with.

2.2 Proposed Method

The proposed image tampering detection consists of five main phases: reading dataset, Pre-processing, feature extraction, and selection, training, and testing, as well as classification. Each phase contains some stages within, **Fig.5** shows the general farmwork of the proposed system.

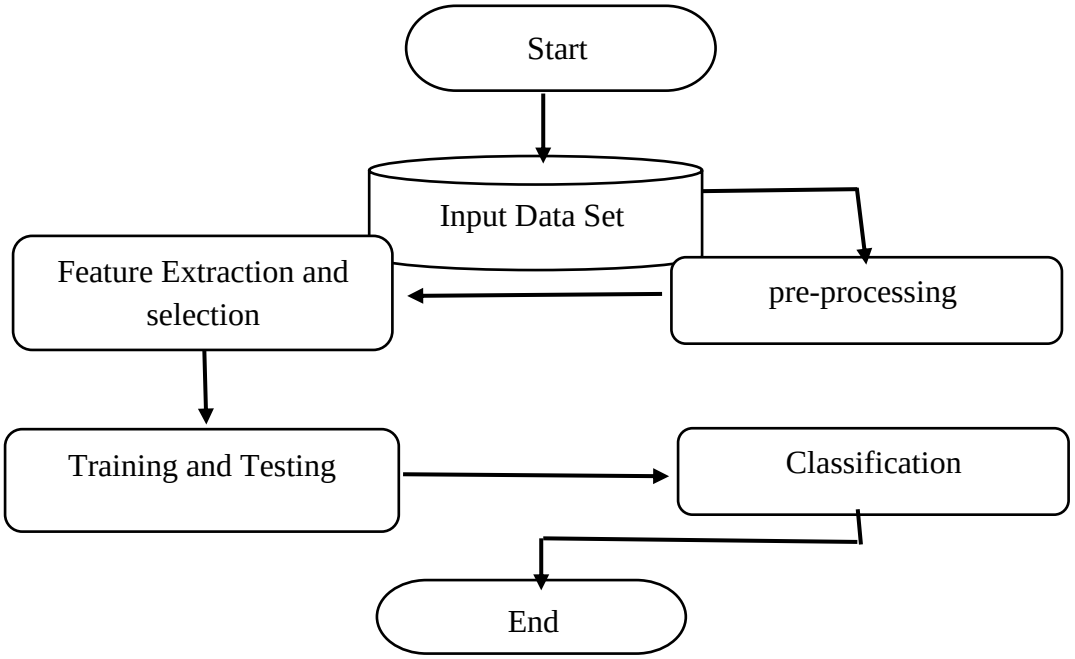

Figure 5: Block diagram of the proposed work

Phase one: reading the contents of the MICC-F2000 input dataset

Phase two: consists of two stages; image resizing and conversion to another domain as in follow: resizing means all input images are unified with standard size 256 I am running a few minutes late; my previous meeting is running over. 256. Conversion means transforming the

RGB image into the YCbCr domain and the YCbCr **(Saleem and El Abbadi, 2020)** image then splinted into three bands **(Reddy et al., 2016)**; the Luminance component (Y), Chrominance component (Cb), and Chrominance component (Cr) have been used the Y image, Cb image, and Cr image respectively **(Koju and Joshi, 2015),** Eqs (1), (2) and (3) where R, B, and G are Red, Blue, and Green **(Ali and Mahdi, 2020)**

$$Y = YCbCr\ 99 * R + 0.587 * G + 0.114 * B \quad (1)$$

$$Cb = 0.492(B - Y) \quad (2)$$

$$Cr - 0.877(R - Y) \quad (3)$$

Phase three: The YCbCr image yields from phase two will be processed into two main stages: Stage one it represents feature extraction and selection for each image in the input dataset. There are three scenarios implemented in this proposed system to detect the forgery. Two statistical functions are used as image features; STD and ASM; and they are used within LBP and MLBP algorithms. STD and ASM images are used as input for (LBP) with one level and MLBP with multiple levels to capture the image's features. The number of features completely depends on the number of levels and the scenario that is implemented by Eq.s (4) (5)(6)**(Huang et al., 2016).**

$$\text{ASM} = \sum_{i,j=1}^{n,m} p_{(i,j)}^2 \quad (4)$$

where P is the pixel of the image.

$$\text{Energy} = \sqrt{\text{ASM}} \quad (5)$$

$$S = \sqrt{\frac{\sum(X-\mu)^2}{n-1}} \quad (6)$$

where S is the standard deviation value, n is the number of data points in the dataset X is: Value of the point in the dataset, and μ is the mean value.

Stage two is normalized for each image by shifting and scaling values to make them range between 0 and 1. The Min-Max algorithm is used to unify the rang value in this stage by Eq. (7) **(Pennington and Spanu, 2015)**.

$$\grave{N} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (7)$$

where Xmax is the feature's maximum value Xmin: is the feature's minimum value N: Normalization value.

Phase four: it is a training and testing process implemented in this phase by taking the features of each image based on a cross-validation approach.

Phase five**:** Using one of the Machine Learning (ML) algorithms where ML **(Chauhan et al., 2019)** is a branch of artificial intelligence **(Alhijaj et al., 2021)** that is widely described as a machine's ability like intelligent human behavior **(Parashar et al., 2018)**. Artificial intelligence systems are used to accomplish complex tasks in a manner comparable to how humans solve problems. In this proposed system, the algorithm used will construct the model based on the given data and this constructed model determines the type of input images. The SVM algorithm is used to classify the data and the outcome of this phase is to classify each image as authentic or forged. **Fig. 6** describes in detail the proposed system implemented in this work.

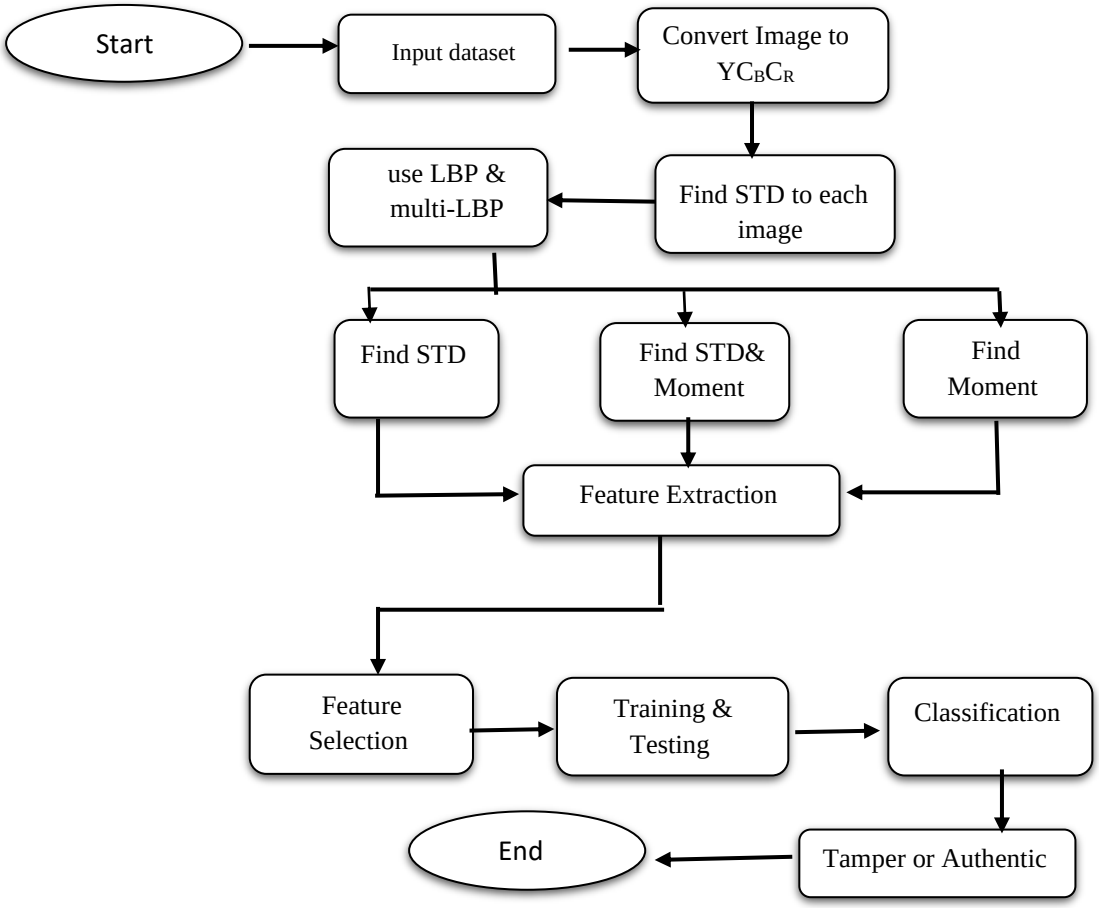

Figure 6. The proposal work system

3. RESULTS AND DISCUSSION

The results of experiments are provided and discussed in this section to assess the effectiveness of proposed systems for Copy-Move Forgery. the evaluation tests have been divided into three parts: (i) the selection mechanism of the classifier. (ii) the performance of the different classifiers with the multi-dataset. (iii)Some of the known fidelity measures (i.e., F-score, Precision ,Accuracy) have been used to assess the quality of the system. (iv) the way used to improve the result performance. There are comprehensive analyses and discussions related to the outcomes achieved via executing each step. The results are described in tables containing the final indication of the detection performance. Finally compares with previous work to justify the obtained results of the proposed system.

As shown in **Fig. 7**, a pre-processing stage is applied to the sample image to convert the 24-bit input color image into a YCbCr image with Resize images. Due to its direct effects on computation time and detection rate, the preceding phase enables Machine Learning (ML) to evaluate the input image accurately.

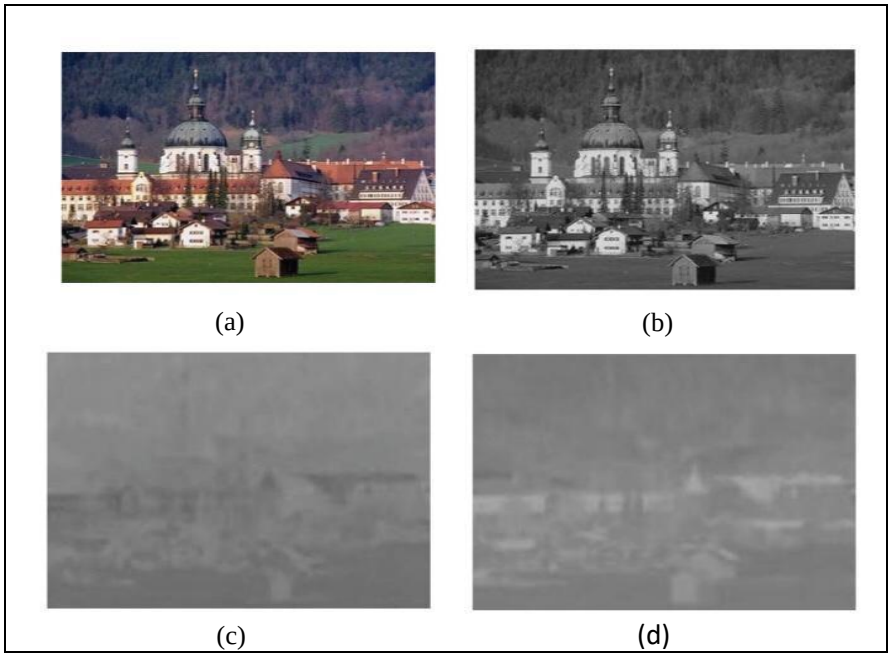

Figure 7. The pre-processing stage (a) RGB image, (b) Luminance component (Y), (c) Chrominance component (Cb), and (d) Chrominance component (Cr)

This phase is considered one of the most important layouts in the system, because features are extracted for each image, and these features will be adopted in the training phase. In the proposed system, three scenarios will be implemented, each scenario has different results due to the use of different types of features, and the three scenario descriptions is listed in the following:

➢ First scenario: MLBP algorithm implemented using the statistical function (ASM), the total features extracted from each image are 900. Since the MLBP has two layouts, it means 450 features are extracted from each layout.

➢ Second scenario: The statistical function (STD) is used to achieve a higher rate of accuracy. STD was used in conjunction with MLBP to extract 900 features where 450 features were extracted individually in each level.

➢ Third scenario: it implements using two statistical functions ASM and STD with the LBP algorithm. However, the number of features extracted is 900 features, 450 with the STD function, and 450 from the ASM function. **Fig. 8** shows an example of the Local Binary Pattern algorithm (LBP).

A normalization process was used max-min algorithm was executed to normalize so that all values are within a certain limit. The extracted features for each image are stored as a vector, it needs processing since the extracted features have a large difference from other features. Subsequently, all values in the CSV file are the file that saved all the features extracted from the previous stage. The length of the vector depends on the number of features that have been extracted from each image and must be within a certain limit for later processing. **Fig. 9** shows the normalization applied with two types of images, tampered and authentic from the same datasets and the histogram with the features of two images from the MICCF2000 dataset

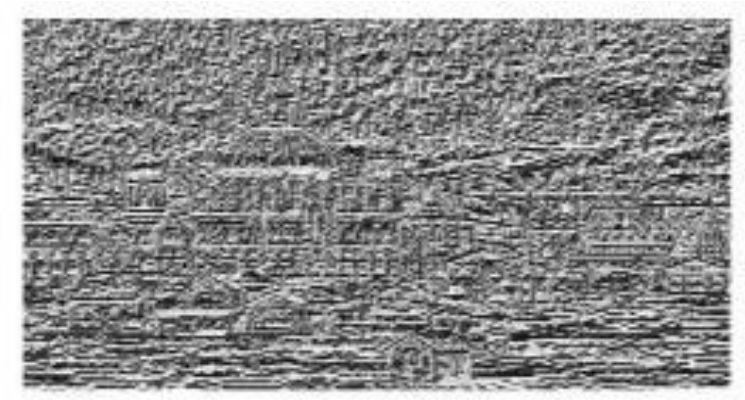

Figure 8. The Local Binary Pattern (LBP) stage

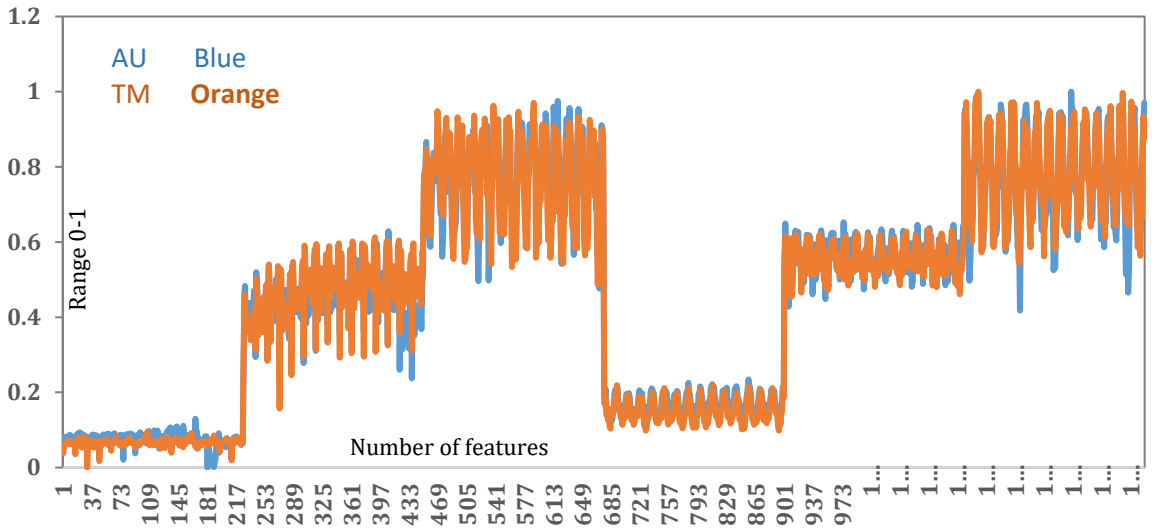

Figure 9. The Normalization Algorithm

Several experiments were performed on the proposed system to evaluate the training and testing model. Among these tests are used to give a decision if the test image is authentic or tampered with the convolution matrices are used to evaluate the system's work, and the results will be explained in tables and figures. Here, more than one scenario and more than one statistical function were used, and many algorithms, namely MLBP and LBP. Several measures are used to know the accuracy of the system. **Table 1** shows the various accuracy rates obtained depending on the number of features, and the number of levels for the SVM classifier with the MICCF2000 dataset **(Silva et al., 2015)**. Additionally, this table reveals the accuracy value with one and two levels implemented by the LBP algorithm. The different scenarios implemented with LBP and MLBP, as well as statistical functions STD and ASM, and the number of LBP features was 450 . Regarding MLBP, there are 900 features per level from each image. Table 1 shows the various accuracy rates obtained depending on the number of features and the number of levels for the SVM classifier with the MICCF2000 dataset**. Table 1.** demonstrates the accuracy value with one and two levels implemented by the LBP algorithm.

Table 1. Accuracy with SVM Classifier

Function	Number of features	Number of Levels	Algorithm	Accuracy %
ASM	450	One level	LBP	97.0
ASM	900	Two level	MLBP	97.5
STD	450	One level	LBP	97.4
STD	900	Two level	MLBP	97.8
STD&ASM	900	One level	LBP	97.8

Fig.10 show the different accuracy rate that has been achieved with the three scenarios that were applied.

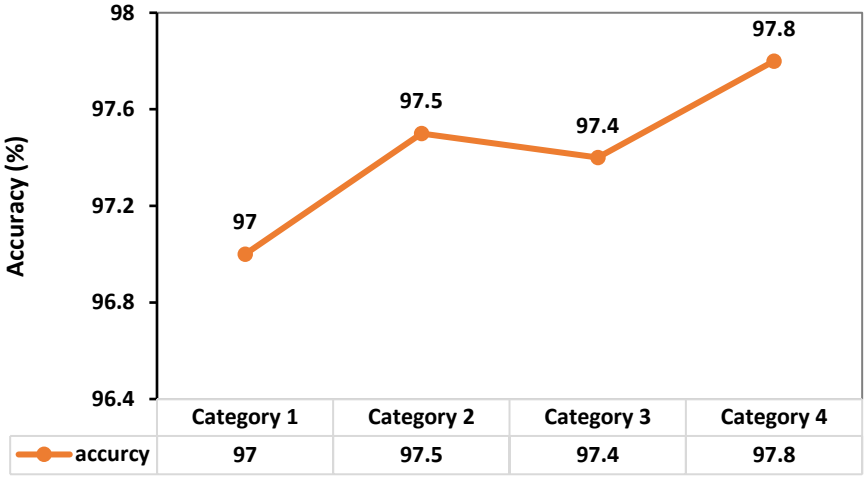

Figure 10. Accuracy of the SVM algorithm

The majority of current measurements depend on the classifier's order to identify classes accurately **(Ahmed and George, 2022)**. The learning algorithms and the classifiers they produce may be evaluated in various ways in machine learning. There is more than one method or measure used to measure the performance of the ML model **(Srivastava and Yadav, 2021).**

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \quad (8)$$

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

$$Recall = \frac{TP}{TP+FN} \quad (10)$$

$$AF1 - score = 2 \cdot \frac{Precision * Recall}{Precision * Recall} \quad (11)$$

$$\text{Sensitivity} = \frac{TP}{TP+FN} \quad (12)$$

$$\text{Specificity} = \frac{TN}{TN+FP} \quad (13)$$

where TP: True Positive, TN: True Negative, FP: False Positive, and FN: False Negative for example, TP means it is correctly detected and it is authentic images **(Balajee and Venkatesh, 2019)**.TN means it is correctly detected and it is tampering images, FP it means incorrect detection and it is tampering images, and FN it is it means incorrect detection and it is authentic images **(Darand et al., 2017)**. It used 450 features extracted from each image that has used ASM feature as clarified in Table 2, the performance metrics in percentage rate. To improve the accuracy, the MLBP algorithm was implemented and used ASM, with two levels where each level extracts 450 features, and then the total feature extracted is 900.

Table 2. The evaluation for one-level and two-level ASM

Evaluation	ASM one level	ASM two-level
Precision (%)	96.0	99.0
Recall (%)	98.0	98.0
F1-score (%)	97.0	97.0
Sensitivity	98.0	98.0
Specificity	96.0	95.0

STD is utilized to achieve a higher rate of accuracy compared to the statistical function ASM used in the first scenario. The same methodology implemented in the previous scenario is adopted in this scenario based on one and two levels of LBP with the SVM algorithm. This implement achieves a higher rate of accuracy than the first statistical function and **Table 3.** demonstrates the obtained results from this scenario.

Table 3. The evaluation for one-level and two-level STD

Evaluation	STD one level	STD two-level
Precision	96.0	97.0
Recall	98.0	98.0
F1-score	97.0	98.0
Sensitivity	97.0	98.0
Specificity	95.0	94.0

To improve the outcomes by achieving a high rate of accuracy where high precision is achieved with fewer steps and in less time, STD and ASM were combined as statistical functions. Moreover, 900 features were extracted from each image using LBP and SVM. **Table 4.** presents the most significant result obtained. SVM was used, giving the best results because the fit process is fair, as the data is categorized in training, which leads to the accuracy rate in the system being higher than the accuracy rate when using another algorithm classifier algorithm.

Table 4. The evaluation with ASM & STD two-level

Evaluation	Value (%)
Precision	97.0
Recall	98.0
F1-score	98.0
Sensitivity	96.0
Specificity	95.0

For the sake of comparison between the present work and some related works, the results of the verification of image manipulation have varied over the years. **Table 5.** lists the accuracy results for tempering image detection of the proposed method and related work. Despite all the good results of the detection or classification mentioned in **Table 5.** Relatively noticeable differences are observed between the currently adopted method and that of other related work. This indicates the efficiency of the adopted method and the correctness of the adopted methodology, besides the correct path of calculations leading to respectful results of tempering detection in images. Following this, the data were classified using three distinct types of classifiers, and **Table 6.** shows the list of the samples of the algorithms that are used in this proposed system.

Table 5. The Results Validation

Reference	Methodology	Accuracy (%)
(Chang et al., 2013)	LBP	95.0
(Manu and Mehtre, 2016)	DCT and ORB	96.0
(Zhang et al., 2018)	DWT and SVM	89%
(Dhivya et al., 2020)	SURF	95.0
(Solaiyappan and Wen, 2022)	SVM, RF, DT	97.0
Proposed System	SVM	97.8

Table 6. the list of samples

no	Sample	Mean
1	LBP	Local Binary Pattern
2	STD	Stander Deviation
3	ASM	Angler Second Moment
4	ML	Machine Learning
5	SVM	Support Vector Machine
6	TP	True Positive
7	TN	True Negative
8	FP	False Positive
9	FN	False Negative

6. CONCLUSIONS

Several results and conclusions were assigned during this work's accomplishment of the best image tampering detection model, from which they can be abstracted. Converting the image from RGB color bands to individual YCbCr color bands facilitates subsequent operations on the image. All images employ three color components. On a grey image, the LBP method describes the relationship between each pixel in the sample image and its neighbor, thereby enhancing the feature extraction process, and extracting the features by dividing the image into non-overlapping blocks and calculating the Angular Second Moment and Standard Deviation (STD) for each block. The number of utilized features depends on the levels employed in the work. We select the most accurate features for each image using a function that selects the most accurate features. After obtaining the features, multiple algorithms were used to construct the model through the training procedure. Then, the testing process was conducted, in which multiple algorithms were applied to the search data, the data was

extracted without labels, and the accuracy of the employed algorithms was evaluated. The different accuracy rates were obtained for each. The difference between the workbooks is also attributable to the number of different levels and features varying from level to level. The accuracy achieved with discovering copy-move was 97.8%.

NOMENCLATURE

Symbole	Description	Symbole	Description
A	Area, m^2.	α	Altitude angle, deg.
T	Time, s	B	Factor of variation, Dimensionless.
T_a	Ambient temperature, ^0C		

Acknowledgements

We would like to thank (Baghdad University, College of Science, Computer Science) for thrie support by the Project copy move image forgery detection using multi-level local binary pattern algorithm and using program (python).

Credit Authorship Contribution Statement

Marwa Emad Mahdi: Writing – review, Software, Methodology of the paper. Nada Hussein M. Ali: Writing – review & editing, original draft, Validation, Software, Methodology**.**

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Ali, N.H.M., and Mahdi, M.E., 2020. Detecting similarity in color images based on perceptual image hash algorithm. IOP Conference Series: *Materials Science and Engineering*, 737, P. 012244. Doi:10.1088/1757-899x/737/1/012244.

Abdalla, Y., Iqbal, M., and Shehata, M., 2017. Copy-move forgery detection based on enhanced patch-match. *International Journal of Computer Science Issues*, 14(6), pp. 1–7. Doi:10.20943/01201706.17

Abdul Hossen , A.M., Ogla , R.A.A. ., Ali , M.M., and Ali , M.M., 2022. Face Detection by Using OpenCV's Viola-Jones Algorithm based on coding eyes. *Iraqi Journal of Science*, 58(2A), pp. 735–745. Doi:10.24996/ijs.2023.64.2.40.

Abdul-Samad, S.T., and Kamal, S., 2020. Image Retrieval Using Data Mining Technique. *Iraqi Journal of Science*, 61(8), pp. 2115–2125. Doi: 10.24996/ijs.2020.61.8.26.

Abidin, A.B.Z., Majid, H.B.A., Samah, A.B.A., and Hashim, H.B., 2019. Copy-move image forgery detection using deep learning methods: a review. *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. Doi:10.1109/icriis48246.2019.9073569.

Agarwal, V., and Mane, V., 2016. Reflective SIFT for improving the detection of copy-move image forgery. In: *IEEE*. 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), 28(3), P. 939. Doi:10.1109/ICRCICN.2016.7813636

Ahmed, A.H.., and George, L.E., 2022. The use of wavelet, DCT & and quadtree for images color compression. *Iraqi Journal of Science*, 58(1C), pp. 550–561. Doi:10.24996/ijs.2023.64.2.37.

Akram, A., Ramzan, S., Rasool, A., Jaffar, A., Furqan, U., and Javed, W., 2022. Image splicing detection using discriminative robust local binary pattern and support vector machine. *World Journal of Engineering*, *19*(4), pp. 459-466. Doi:10.1108/WJE-09-2020-0456

Al-Bayati, A.Q., Al-Araji, A.S., and Ameen, S.H., 2020. Arabic sentiment analysis (ASA) using deep learning approach. *Journal of Engineering*, 26(6), pp. 85–93. Doi:10.31026/j.eng.2020.06.07.

Alhijaj, T.B., Hameed, S.M., and Attea , B.A., 2021. A decision tree-aware genetic algorithm for botnet detection. *Iraqi Journal of Science*, (7), pp. 2454–2462. Doi:10.24996/ijs.2021.62.7.34.

Al-Qershi, O.M., and Khoo, B.E., 2013. Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International*, 231(1-3), pp. 284–295. Doi:10.1016/j.forsciint.2013.05.027.

Alshibani, D.R., and Sadeq, Z., 2018. Image content verification based on DWT and chaotic map watermarking. *Iraqi Journal of Science*, 59(1C), pp. 607–616. Doi: 10.24996/ijs.2020.61.7.37.

Anbu, T., Joe, M.M., and Murugeswari, G., 2020 . A comprehensive survey of detecting tampered images and localization of the tampered region. *Multimedia Tools and Applications*, 80(2), pp. 2713–2751. Doi:10.1007/s11042-020-09585-z

Asghar, K., Habib, Z. Hussain, M., 2017. Copy-move and splicing image forgery detection and localization techniques: a review. *Australian Journal of Forensic Sciences*, 49(5), pp. 281-307. Doi:10.1007/s11042-030-09553

Babu, S.T., and Rao, C.S., 2022. An optimized technique for copy–move forgery localization using statistical features. *ICT Express*, *8*(2), pp. 244-249. Doi:10.1016/j.icte.2021.08.016.

Balajee, R.M., and Venkatesh, K., 2019. A survey on machine learning algorithms and finding the best out there for the considered seven medical data sets scenario. 12(6), pp. 3059–3059. Doi:10.5958/0974-360x.2019.00518.3.

Birajdar, G.K., and Mankar, V.H., 2013. Digital image forgery detection using passive techniques: A survey. *Digital Investigation*, 10(3), pp.226–245.Doi:10.1016/j.diin.2013.04.007.

Chang, J., Chen, B. H., and Tsai, C. S., 2013. LBP-based fragile watermarking scheme for image tamper detection and recovery. *IEEE International Symposium on Next-Generation Electronics*. 4(13), pp. 173-176. Doi:10.1109/isne.2013.6512330.

Chauhan, V.K., Dahiya, K., and Sharma, A., 2019. Problem formulations and solvers in linear SVM: a review. *Artificial Intelligence Review*, *52*(2), pp.803-855. Doi:10.1007/s10462-018-9614-6.

Cozzolino, D., Poggi, G., and Verdoliva, L., 2015. Efficient dense-field copy–move forgery detection. *IEEE Transactions on Information Forensics and Security*, 10(11), pp. 2284–2297. Doi:10.1109/tifs.2015.2455334.

Darand, M., Amanollahi, J., and Zandkarimi, S., 2017. Evaluation of the performance of TRMM Multi-satellite Precipitation Analysis (TMPA) estimation over Iran. *Atmospheric Research*, 190, pp. 121–127. Doi:10.1016/j.atmosres.2017.02.011

Dhir, V., 2017. A review on image forgery & its detection procedure. *International Journal of Advanced Research in Computer Science*, *8*(4), pp. 140-148. Doi:10.26483/ijarcs.v8i4.4162.

Dhivya, S., Sangeetha, J., and Sudhakar, B., 2020. Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique. *Soft Computing*, 24(19), pp. 14429–14440. Doi:10.1007/s00500-020-04795-x.

Hamid, I. I., and Jamel, E. M., 2022 . Image Watermarking using Integer Wavelet Transform and Discrete Cosine Transform. *Iraqi Journal of Science*, 57(2B), pp. 1308–1315. Doi:10.24996/ijs.2020.61.12.43.

Hassan, J.M., and Moayed, M.W., 2023. the effect of hydraulic accumulator on the performance of hydraulic system. *Journal of Engineering*, 20(7), pp. 174–190. Doi: 10.31026/j.eng.2014.07.12.

Hassoon, A.S., and Jalil, L.F., 2022. Classification of Iraqi Anber rice by using image processing and KNN algorithm. *Iraqi Journal of Science*, 58(2A), pp. 716–725. Doi:10.24996/ijs.2023.64.2.41.

Huang, L., Chen, C., Li, W., and Du, Q., 2016. Remote sensing image scene classification using multi-scale completed local binary patterns and fisher vectors. *Remote Sensing*, 8(6), pp. 483- 490. Doi:10.3390/rs8060483.

Huang, S., Cai, N., Pacheco, P.P., Narrandes, S., Wang, Y., and Xu, W., 2018. Applications of support vector machine (SVM) learning in cancer genomics. *Cancer genomics & proteomics*, *15*(1), pp. 41-51. Doi:10.20922/01201603.15

Ibrahim, A., George, L.E., and Hassan, E.K., 2020. Color Image Compression System by using Block Categorization Based on Spatial Details and DCT Followed by Improved Entropy Encoder. *Iraqi Journal of Science*, 61(11), pp. 3127–3140. Doi: 10.24996/ijs.2020.61.11.32.

Jaiswal, A., and Srivastava, R., 2020. A technique for image splicing detection using hybrid feature set. *Multimedia Tools and Applications*, 79(17). pp. 11837–11847.Doi:10.1007/s11042-019-08480-6.

Kaur, R., 2016. Image forgery and detection of copy move forgery in digital images: a survey of recent forgery detection techniques. *International Journal of Computer Applications*, 139(5), pp. 39–47. Doi:10.5120/ijca2016909164.

Koju, R., and Joshi, S.R., 2015. Comparative analysis of color image watermarking technique in RGB, YUV, and YCbCr Color channels . *Nepal Journal of Science and Technology*, 15(2), pp. 133–140. Doi:10.3126/njst.v15i2.12130.

Kumar, M., and Srivastava, S., 2017. Image forgery detection based on physics and pixels: a study. *Australian Journal of Forensic Sciences*, 51(2), pp. 119–134. Doi:10.1080/00450618.2017.1356868.

Lin, C., Lu, W., Huang, X., Liu, K., Sun, W., Lin, H., and Tan, Z. , 2018 . Copy-move forgery detection using combined features and transitive matching. *Multimedia Tools and Applications*, 78(21), pp. 30081–30096. Doi:10.1007/s11042-018-6922-4.

Manu, V.T., and Mehtre, B.M., 2016. Detection of copy-move forgery in images using segmentation and SURF. *Advances in intelligent systems and computing.*5(9), pp. 645–654. Doi:10.1007/978-3-319-28658-7_55.

Musaed, A., 2016. Image tampering detection based on local texture descriptor and extreme learning machine. International Conference on Computer Modelling and Simulation, 10(3), pp. 507-518. Doi:10.1109/uksim.2016.39.

Parashar, A., Upadhyay, A.K., and Gupta, K., 2018. An effectual classification approach to detect copy-move forgery using support vector machines. *Multimedia Tools and Applications*, 78(20), pp. 29413–29429. Doi.org/10.1007/s11042-018-6707-9.

Pennington, H.G., Li, L., and Spanu, P.D., 2015. Identification and selection of normalization controls for quantitative transcript analysis in Blumeria graminis. *Molecular Plant Pathology*, 17(4), pp .625–633. Doi:10.1111/mpp.12300.

Prinkle, R., and Jyoti, R., 2015. Copy-move forgery attack detection in digital images. *International Journal of Engineering Research*, 4(06), pp 1211-1217. Doi:10.17577/ijertv4is061110.

Reddy, R.V.K., Raju, K.P., Kumar, L.R. and Kumar, M.J., 2016. Grey level to RGB using YCbCr color space Technique. *International Journal of Computer Applications*, *147*(7), pp. 25– 28. Doi:10.5120/ijca2016911180

Saleem, E. ., and El Abbadi, N. K., 2020 . Auto colorization of gray-scale image using ycbcr color space. *Iraqi Journal of Science*, 61(12), pp. 3379–3386. Doi:10.24996/ijs.2020.61.12.26.

Salih, M. M., Ahmed, M. A., Al-Bander, B., Hasan, K. F., Shuwandy, M. L., and Al-Qaysi, Z., 2023. Benchmarking framework for COVID-19 classification machine learning method based on fuzzy decision by opinion score method. *Iraqi Journal of Science*, 64(2), pp. 922–943. Doi:10.24996/ijs.2023.64.2.36.

Silva, E., Carvalho, T., Ferreira, A., and Rocha, A., 2015. Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. *Journal of Visual Communication and Image Representation*, 29(8), pp. 16–32. Doi:10.1016/j.jvcir.2015.01.016.

Solaiyappan, S., and Wen, Y., 2022. Machine learning based medical image deepfake detection: A comparative study. *Machine Learning with Applications*, 8(15), P.100298. Doi:10.1016/j.mlwa.2022.100298.

Srivastava, V., and Yadav, S.K. , 2021. Digital image tampering detection using multilevel local binary pattern texture descriptor. *Journal of Applied Security Research*, 17(1), pp. 62–79. Doi:10.1080/19361610.2021.1883397

Suresh, G., and Rao, C.S., 2016. Copy move forgery detection using glcmbased statistical features. *International Journal on Cybernetics & Informatics (IJCI)*, *5*(4), P.165. Doi:10.1010/s10462-017-8614-8.

Thakur, T., Singh, K., and Yadav, A., 2018. Blind approach for digital image forgery detection. *International Journal of Computer Applications*, 179(10), pp. 34–42. Doi:10.5120/ijca2018916108.

Wang, C., Zhang, Z., and Zhou, X., 2018. An image copy-move forgery detection scheme based on A-KAZE and SURF features. *Symmetry*, *10*(12), P.706. Doi:10.1008/s11042-018-54320.

Wu, Y., Abd-Almageed, W., and Natarajan, P., 2018. BusterNet: detecting copy-move image forgery with source/target localization. *Computer Vision – ECCV 2018,16(7)*, pp. 170–186. Doi:10.1007/978-3-030-01231-1_11.

Zhang, Q., Lu, W., Wang, R., and Li, G., 2018. Digital image splicing detection based on markov features in block DWT domain. *Multimedia Tools and Applications*, 77(23), pp. 31239–31260. Doi:10.1007/s11042-018-6230-z.