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.iq1, nada.husn@sc.uobaghdad.edu.iq2

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, Stannder Deviation (STD) and Angular 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.
كشف تزوير نسخ الصور باستخدام خوارزمية النمط الثنائي المحلي متعدد المستويات

مروه عمام مهدي 1، حسن محمد علي 2
قسم الحاسوب، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة

أصبح التلاعب بالصور الرقمية سائداً بشكل متزايد بسبب التوفر الواسع لأدوات تحرير الصور المتقدمة. في تزييف نقل النسخ، يتم نسخ جزء من الصورة وصقه في منطقة أخرى داخل نفس الصورة. تبدأ المنهجية المقترحة باستخراج ميزات خوارزمية LBP للنمط الثنائي المحلي من الصورة. يتم حساب وظائف إحصائيتين رئيسيتين STD و ASM لكل ميزة LBP، مع التقاط معلومات إحصائية إضافية حول القوام المحلي. بعد ذلك، يتم تطبيق تحديد الميزات المتعددة 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. في اكتشاف Copy-Move، تُستخدم القطع الأثرية وخصائصها كميزات للصورة، و Support و Copy Move. نتائج الاكتشاف تعود إلى النهج التعلم الآلي. تم استخدام مجموعة بيانات فريدة من كل تطبيق وتم اختبار كل مصنف، والذي هو معركة الأنظمة التموينية التي تم تصميمها بواسطة أعضاء الفريق. وبالتالي، اكتشف هذا الالتزامات التجريبية فعالية النمطية المقترحة في اكتشاف نقل النسخ. أُسفرت مرحلة الاختبار عن نتائج متناقضة. في حالة أفضل سيناريو، تم تشفير النتيجة وتقييمها، وتم تحديد تجربة متعددة. حصلت 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
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 utilization 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 tums, 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.

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.

![Splicing image](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.

![Retouched image](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, Preprocessing, 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](image)

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 (Koku and Joshi, 2015). Eqs (1), (2) and (3) where R, B, and G are Red, Blue, and Green (Ali and Mahdi, 2020).

\[ Y = YCbCr \times 99 * R + 0.587 * G + 0.114 * B \]  
(1)

\[ Cb = 0.492(B - Y) \]  
(2)

\[ Cr = 0.877(R - Y) \]  
(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).

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

where P is the pixel of the image.

\[ \text{Energy } = \sqrt{\text{ASM}} \]  
(5)

\[ S = \sqrt{\frac{\sum (X-\mu)^2}{n-1}} \]  
(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 \( \mu \) 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).

\[ \hat{X} = \frac{X-X_{\text{min}}}{X_{\text{max}}-X_{\text{min}}} \]  
(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.
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.
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.
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

<table>
<thead>
<tr>
<th>Function</th>
<th>Number of features</th>
<th>Number of Levels</th>
<th>Algorithm</th>
<th>Accuracy %</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASM</td>
<td>450</td>
<td>One level</td>
<td>LBP</td>
<td>97.0</td>
</tr>
<tr>
<td>ASM</td>
<td>900</td>
<td>Two level</td>
<td>MLBP</td>
<td>97.5</td>
</tr>
<tr>
<td>STD</td>
<td>450</td>
<td>One level</td>
<td>LBP</td>
<td>97.4</td>
</tr>
<tr>
<td>STD</td>
<td>900</td>
<td>Two level</td>
<td>MLBP</td>
<td>97.8</td>
</tr>
<tr>
<td>STD&amp;ASM</td>
<td>900</td>
<td>One level</td>
<td>LBP</td>
<td>97.8</td>
</tr>
</tbody>
</table>

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

![Image of accuracy graph](attachment:image.png)

**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](#)).

\[
\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN} \tag{8}
\]

\[
\text{Precision} = \frac{TP}{TP + FP} \tag{9}
\]

\[
\text{Recall} = \frac{TP}{TP + FN} \tag{10}
\]

\[
\text{AF1 - score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{11}
\]

\[
\text{Sensitivity} = \frac{TP}{TP + FN} \tag{12}
\]

\[
\text{Specificity} = \frac{TN}{TN + FP} \tag{13}
\]
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 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

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>ASM one level</th>
<th>ASM two-level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision (%)</td>
<td>96.0</td>
<td>99.0</td>
</tr>
<tr>
<td>Recall (%)</td>
<td>98.0</td>
<td>98.0</td>
</tr>
<tr>
<td>F1-score (%)</td>
<td>97.0</td>
<td>97.0</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>98.0</td>
<td>98.0</td>
</tr>
<tr>
<td>Specificity</td>
<td>96.0</td>
<td>95.0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>STD one level</th>
<th>STD two-level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td>96.0</td>
<td>97.0</td>
</tr>
<tr>
<td>Recall</td>
<td>98.0</td>
<td>98.0</td>
</tr>
<tr>
<td>F1-score</td>
<td>97.0</td>
<td>98.0</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>97.0</td>
<td>98.0</td>
</tr>
<tr>
<td>Specificity</td>
<td>95.0</td>
<td>94.0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>Value (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td>97.0</td>
</tr>
<tr>
<td>Recall</td>
<td>98.0</td>
</tr>
<tr>
<td>F1-score</td>
<td>98.0</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>96.0</td>
</tr>
<tr>
<td>Specificity</td>
<td>95.0</td>
</tr>
</tbody>
</table>
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

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

Table 6. the list of samples

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

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**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Area, $m^2$.</td>
<td>$\alpha$</td>
<td>Altitude angle, deg.</td>
</tr>
<tr>
<td>T</td>
<td>Time, s</td>
<td>B</td>
<td>Factor of variation, Dimensionless.</td>
</tr>
<tr>
<td>$T_a$</td>
<td>Ambient temperature, °C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**


