الكشف عن تزوير الصور الرقمية باستخدام منهجية متكيفة ومُحسَّنة

د. محمد بسام الكردي*
رنيم طاسية **

(تاريخ الإيداع 15 / 7 / 2020. قُبِل للنشر في 1/ 2 / 2021)

□ ملخّص □

الدراسة المقدمة من خلال هذا البحث تهتم بموضوع الصور الرقمية، وهي موجهة بشكلٍ خاصٍ للكشف عن التزوير الذي يمكن أن يتم تطبيقه على الصور الرقمية. إن النظام المُقترح يقدم تطبيقاً ديناميكياً متكيفاً، يستطيع الكشف عن النوعين الأكثر انتشاراً واستخداماً من التزوير وهما: تزوير النسخ، وتزوير الدمج. حيث يمكن من خلال هذا النظام الكشف عن هذين النوعين من التزوير، وذلك في أنواع وأحجام مختلفة من الصور، على عكس العديد من الدراسات السابقة والتي كانت مخصصة لنوع تزوير معين أو لصورة بمقاييس وشروط محددة. يقوم التطبيق بشكل ديناميكي بالتكيف مع الصورة المُعطاة، واختيار الخوارزمية التي تلائم هذه الصورة، بحيث يتم التوصل إلى النتيجة الأفضل في الكشف عن التزوير وذلك بما يناسب معطيات الصورة وخصائصها.

كما يقدّم النظام المقترح تحسيناً فيما يتعلق بعدد الإنذارات الخاطئة التي كانت تصدر عن الأنظمة الأساسية التي يعتمد عليها التطبيق في الكشف عن تزوير النسخ، حيث أن النظامين الأساسيين المُقدمين في دراسات سابقة، كانا يعانيان من عدد كبير من الإنذارات الخاطئة والتي كانت تُظهر وجود تزوير في حين أن الصورة أصلية غير مزورة. لذلك كان أحد أهداف هذه الدراسة هو البحث عن أسباب هذه الإنذارات الخاطئة في كل طريقة على حدة، ومعالجة هذه الأسباب بهدف تحسين أداء الخوارزميات الأصلية.

الكلمات المفتاحية: تزوير الدمج؛ تزوير النسخ؛ تحويل DCT؛ خوارزمية SURF؛ المصفوفة CFA.

* أستاذ – الجامعة الافتراضية السورية – سورية.
** طالبة دراسات عليا (ماجستير) – قسم علوم الوب – الجامعة الافتراضية السورية – سورية.

Image Forgery Detection Using an Adaptive and Improved Methodology

Dr. Mohamad-Bassam Kurdy [*]
Raneem Tassia [**]

(Received 15 / 7 / 2020. Accepted 1 / 2 / 2021)

□ ABSTRACT □

The study presented through this research deals with the subject of digital images, it is specifically directed to detect forgery that can be applied to digital images. The proposed system provides an adaptive and dynamic application, which can detect the two most common and used types of forgery: Splicing forgery, and Cloning (copy-move) forgery. This system can detect these two types of forgery, in different types and sizes of images. Unlike many previous studies that were intended for a specific type of forgery, or for an image with specific characteristics and conditions. The application dynamically adapts to the given image and selects the optimal algorithm that fits image, so to arrive to the best result in detecting the forgery as perceived by the image data and specifications.

The proposed system also provides improvement concerning the number of false alarms (False Positive), that were issued by the basic systems that detect Cloning forgery. As the two basic systems presented in previous studies were suffering from a large number of false alarms, that showed the existence of fraud while the original image was not forged. Therefore, one of the aims of this study was to search for the causes of these false alarms in each method separately, and to treat these causes so to improve the performance of the original algorithms.

Keywords: Splicing Forgery; Cloning Forgery; DCT; SURF; CFA.

[*] **Professor, Syrian Virtual University, Syria.**
[**] **Postgraduate Student (Master), Department of Web Science, Syrian Virtual University, Syria.**

مقدمة:

نادراً ما يخلو أي مجال من مجالات الحياة في عصرنا الحالي من وجود الصور الرقمية، حيث يتم استخدامها في جميع المجالات تقريباً، كالتصوير الطبي، والصحافة، وأنظمة المراقبة، والتحقيقات الجنائية، ووسائل التواصل الاجتماعي، وغيرها العديد. ومع وجود هذه الأعداد الهائلة من الصور وتوفرها بشكل سهل للجميع، ولأننا نحن البشر نعتقد ونميل إلى تصديق ما نراه بأعيننا، تأتي أهمية التأكيد على صحة وموثوقية هذه الصور.

يتواجد حالياً العديد من برامج معالجة الصور الرقمية (Adobe Photoshop على سبيل المثال لا الحصر)، والتي بدورها تقدم إمكانيات هائلة تمكّن مستخدميها من إجراء تعديلات عديدة على الصور وبشكل سهل وفعال وغير مرئي بالعين المجردة. من هنا تبرز الضرورة والحاجة الملحة لتطوير آليات وأنظمة للكشف عن التزوير الذي قد يحصل، بحيث تكون قادرة على التحقق من صحة هذه الصور، وبالتالي الكشف عن أي تزوير أو تلاعب فيها. لذلك تُعتبر أنظمة كشف التزوير من المجالات الهامة في معالجة الصور والبحث عن أدلة تساعد في إثبات أصالة الصورة نظراً لاستخدام هذه الأخيرة في مناحي الحياة المختلفة وتطبيقاتها التي قد تكون حرجة في بعض الحالات كالمجال الطبي أو التحقيقات الجنائية، والتي قد تؤدي إلى نتائج أو تشخيصات خاطئة تكون عواقبها وخيمة.

وعليه نرجو أن يكون البحث، الذي تم العمل عليه خلال العام المنصرم والعام الحالي، حلاً لحالات سوء الاستخدام، أو الأخطاء غير المقصودة التي قد تطرأ على الصورة الرقمية.

أهمية البحث وأهدافه:

تأتي أهمية هذا البحث كونه يقدم نظاماً قادراً على التحقق من صحة الصورة وكشف التزوير أو التعديل الحاصل عليها، لما للصور من أهمية في العديد من المجالات والتطبيقات. لذلك من الممكن الاستفادة من هذا النظام إما للاستخدامات الشخصية بغية التحقق من دقة المعلومات المقدمة لنا، وخصوصاً في ظل وسائل التواصل الاجتماعي الحديثة والتي جعلت الصور جزءاً أساسيا منها. أو من خلال تطبيقه لدى الجهات التي تعتمد في بنيتها وعملها وفي اتخاذ قراراتها على المعلومات الموجودة في الصور كمجالات الرعاية الصحية والتحقيقات الجنائية وأنظمة المراقبة والتصوير الصحفي وغيرها العديد.

قد تبين من خلال الدراسة المرجعية التي قمنا بها للأبحاث السابقة والتي كانت تهتم بموضوع الكشف عن تزوير الصور الرقمية، أن معظم هذه الأبحاث كانت تعنى بالكشف عن نوع محدد من التزوير بغض النظر عن الأنواع الأخرى. تهتم الدراسات المقدمة من خلال الأبحاث **[1]** و**[2]** بالكشف عن تزوير الدمج فقط (Splicing Forgery)، في حين أن الدراسات **[3]** و**[4]** تقدم دراسة حول الكشف عن تزوير النسخ (Cloning Forgery).

كما تبين أن الدراسة المقدمة من خلال البحث **[5]** أنه يستطيع الكشف عن أكثر من نوع من التزوير، ولكنه لا يتيح إمكانية تحديد موقع التزوير الحاصل على الصورة.

كما تعاني بعض الأنظمة المقترحة في الدراسات السابقة من بعض القيود المتعلقة بحجم أو دقة الصورة. فمثلا تستطيع الدراسة **[6]** الكشف عن تزوير النسخ بشكل جيد في الصور الكبيرة الحجم والعالية الدقة، في حين تفشل في الكشف عن تزوير الصور الصغير. وعلى العكس فإن الدراسة **[7]** تكشف عن تزوير الصور الصغيرة، بينما يتوقف النظام عن العمل في حال كانت الصورة كبيرة الحجم.

من هنا جاءت أهمية الدمج والمكاملة بين هذه الأنظمة الموجودة بغية تحقيق الاستفادة الأكبر في هذا المجال. يهدف هذا البحث إلى:

- بناء نظام متكامل قادر على الكشف عن التزوير الحاصل في الصورة وذلك للنوعين الأكثر انتشاراً للتزوير.
- العمل على الدمج بين عدة أساليب لأخذ المفيد والجيد منها بعد دراستها ومعرفة الحالة الأنسب والأكثر ملائمة لتطبيق كل منها وذلك بهدف الحصول على نتائج أفضل.
- كشف نقاط الضعف في هذه الأساليب التي تم دمجها والعمل على تحسين نتائجها بغية تحسين أداء النظام ككل.
- جعل النظام متكيف ومتلائم مع جميع أنواع وأحجام الصور وذلك من خلال إضافة خطوات ديناميكية ومتكيفة حسب كل صورة.

النظام المقترح:

تم بناء النظام المقترح اعتماداً على ثلاث دراسات سابقة كان لها فعالية ونتائج جيدة في الكشف عن التزوير الحاصل على الصور الرقمية، دراستان منها موجهتان للكشف عن تزوير النسخ (Cloning or Copy-Move Forgery)، وواحدة مخصصة للكشف عن تزوير الدمج (Splicing Forgery). وهذين النوعين من التزوير هما الأكثر انتشاراً واستخداماً في تزوير الصور.

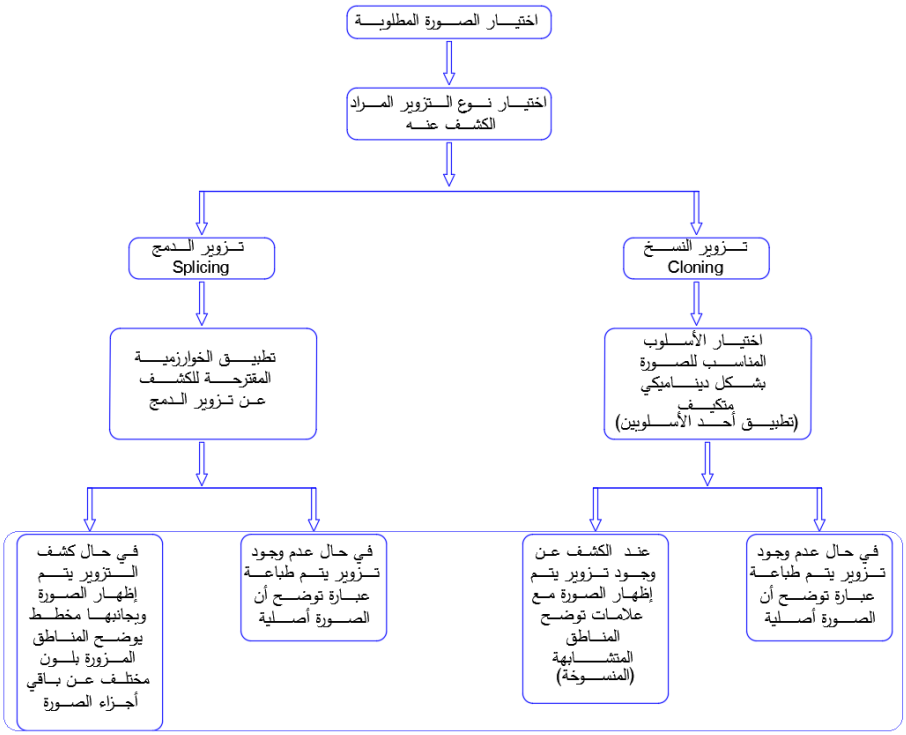
وللتمييز بين هذين النوعين من التزوير بشكل مختصر ومبسط، فإن تزوير الدمج هو التزوير الذي يتم من خلال إدخال جزء من صورة، أو أجزاء من عدة صور، ضمن صورة أخرى لتشكيل صورة مزورة تحوي على معلومات غير صحيحة **[8]**. أما بالنسبة لتزوير النسخ فهو الذي يتم فيه نسخ جزء من الصورة نفسها ولصقه في موضع آخر ضمن الصورة وذلك بهدف إخفاء جزء معين من الصورة أو لتشكيل صورة غير موثوقة تحتوي على معلومات خاطئة**[9]** .

من خلال دراسة وتحليل هذه الدراسات تبيّن أولاً أنها تقدم أنظمة غير متكاملة فيما يخص الكشف عن التزوير، حيث أن كل دراسة منها موجهة للكشف عن نوع محدد من التزوير، كما تبيّن أن هذه الأنظمة لا تستطيع التعامل إلا مع حالات معينة كأن تكون الصور صغيرة الحجم في أحدها، أو أن يتطلب النظام المقدَّم أن تكون الصورة عالية الدقة كي يتمكن من كشف وجود التزوير فيها. كما تبيَّن من خلال دراسة وتحليل هذه الأنظمة أن الخوارزميات المستخدمة للكشف عن تزوير النسخ تعاني من عدد كبير من الإنذارات الخاطئة، التي تبين وجود تزوير في الصورة في حين أنها صورة أصلية.

انطلاقاً من محدودية تلك الأنظمة، وبهدف الوصول إلى نظام متكامل يستطيع الكشف عن النوعين الأكثر انتشاراً من أنواع التزوير المطبقة على الصور الرقمية، قمنا بإضافة خطوات على الخوارزميات الأصلية لسد الثغرات التي يعاني منها كل نظام وتحسين النتائج الصادرة عنه وخصوصاً فيما يتعلق بالإنذارات الخاطئة الناتجة عن النظام، كما قمنا بخلق بيئة متكيفة تقوم بشكل أوتوماتيكي باختيار الأسلوب الأمثل للصورة المُدخلة بالاعتماد على حجمها ونوع نسيجها وبنيتها، لكي نتمكن كنتيجة لهذا العمل من تقديم بيئة عمل متكاملة قدر الإمكان ومتكيفة مع الصورة المُدخلة للكشف عن تزوير الصور الرقمية.

لوصف مراحل عمل النظام فإنه يتم في البداية اختيار الصورة المراد الكشف عن صحتها وتحميلها إلى التطبيق. ليقوم بعدها مستخدم النظام باختيار نوع التزوير المراد الكشف عنه (Cloning or Splicing Forgery Detection). بعد ذلك يتم تطبيق أحد الخوارزميات المُستخدمة في التطبيق على الصورة بحسب نوع التزوير المطلوب الكشف عنه من قبل مستخدم النظام. تكون نتيجة التطبيق إما عبارة توضح أن الصورة أصلية ولم يحصل عليها أي تعديل، أو يقوم

التطبيق بعرض الصورة للمستخدم موضحاً عليها مناطق التزوير بشكل علامات يختلف شكلها ولونها بحسب الأسلوب الذي تم تطبيقه على الصورة وذلك بهدف توضيح التكيف والديناميكية التي يقدمها التطبيق في اختيار الخوارزمية المناسبة للصورة. يبين المخطط التالي الموضح في الشكل (1) الآلية العامة لعمل التطبيق:



الشكل (1): مخطط يوضح الآلية العامة لعمل النظام المُقترح

وسوف نوضح في الفقرات التالية الخوارزمية والأسلوب المتبع عند اختيار الكشف عن كل نوع من التزوير.

1. الكشف عن تزوير الدمج:

عند اختيار الكشف عن تزوير الدمج فإنه يتم تطبيق الخوارزمية المقدمة في الدراسة **[10]**، والتي تكشف عن وجود مناطق في الصورة لا تنتمي إليها بل تم جلبها من صورة أخرى وإدراجها ضمن الصورة في موقع معين.

تعتمد هذه الخوارزمية في أساسها على إيجاد مصفوفة الألوان (Color Filter Array CFA) لأجزاء أو بلوكات الصورة ومن ثم البحث عن وجود عدم تناسق أو تغير في نمط هذه المصفوفات. فالصورة الأصلية تكون كل أجزائها متشابهة ولها نفس مصفوفة الألوان بنمط وترتيب معين وذلك النمط يتعلق بنوع الكاميرا التي التقطت الصورة، وبالتالي فإن وجود خلل أو تغيير لنمط الألوان في جزء من الصورة هو دليل على كون هذا الجزء من صورة أخرى ولا ينتمي إلى الصورة الأصلية. لذلك فإنه يتم تقسيم الصورة إلى بلوكات ويتم إعادة توليد البلوكات بتطبيق فلاتر على الصورة وفق النماذج الأربعة الأساسية (Bayer CFA). يتم بعدها حساب متوسط مربع الخطأ MSE بين البلوك الأصلي والبلوك المعاد توليده لكل نموذج CFA. أحد الأخطاء سيكون أصغر من الثلاثة الباقية بشكل ملحوظ في حال عدم وجود تزوير في الصورة، وتكون القيمة المقابلة لهذا الخطأ هي النموذج الأصلي لمصفوفة ألوان الصورة. ولتحديد موقع التزوير يتم مقارنة جميع نماذج الCFA المستخلصة لجميع البلوكات، فإذا كانت الصورة أصلية فإن جميع أجزائها

تملك نفس مصفوفة الألوان، أما في حال وجود بلوكات مختلفة عن باقي أجزاء الصورة تكون هذه البلوكات من صورة أخرى ولا تنتمي إلى الصورة الأصلية.

وعلى الرغم من بساطة مبدأ هذه الخوارزمية إلا أنها أثبتت فعاليتها في الكشف عن تزوير الدمج بشكل جيد حيث حققت نسبة صحة تعادل 0.9963 كما أن نسبة الإنذارات الخاطئة (False Positive) هي فقط 0.0026 كما هو مبين في الدراسة **[10]**، لذلك تم الاعتماد عليها في التطبيق المقدم في هذا البحث، بالإضافة إلى سرعة أدائها وكلفتها المنخفضة حيث لا تحتاج إلى خوارزمية ذكية لتصنيف النتائج.

2. الكشف عن تزوير النسخ:

عند اختيار الكشف عن تزوير النسخ في الصورة المطلوبة، فإن التطبيق يقوم تلقائياً وبشكل أوتوماتيكي متكيف باختيار أحد أسلوبين مستخدمين في النظام وذلك بحسب ما يناسب الصورة من حيث حجمها وبنيتها وخصائصها. فقد تبين من خلال دراسة الأساليب الأصلية أن كل من الأسلوبين يعمل بشكل جيد ضمن حالة معينة وبشروط محددة، فمثلاً الأسلوب الأول يستطيع الكشف عن التزوير بشكل فعال وبدقة عالية في حال كانت الصورة صغيرة الحجم، أما عند محاولة تطبيقه على صورة كبيرة عالية الدقة فإن هذا النظام يتوقف عن العمل ولا يستطيع تقديم أي نتيجة للمستخدم. وعلى العكس تبين أن الأسلوب الثاني يعمل بشكل فعال وسريع مع الصور العالية الدقة والتي تحتوي على معلومات وبيانات غزيرة في حين أنه لا يستطيع الكشف عن تزوير الصور الصغيرة والتي لا تملك العديد من الخصائص.

كما تبين من خلال تقييم عمل كل من هاتين الخوارزميتين أن كل منها تعاني من مشكلة وجود عدد كبير من الإنذارات الخاطئة التي تُظهر وجود التزوير في حين أن الصورة أصلية وغير مزورة. لذلك قمنا بإضافة عدد من الخطوات أو المراحل على كل خوارزمية منها، هذه الخطوات المُضافة تقلل من الإنذارات الخاطئة بشكل ملحوظ، وتختلف هذه الخطوات من خوارزمية إلى أخرى حسب مبدأ عمل كل منها. وسنوضح فيما يلي آلية عمل كل منهما.

2.1 الأسلوب الأول في الكشف عن تزوير النسخ:

يعتمد هذا الأسلوب بشكل أساسي على الدراسة **[7]**. ويتم فيه تقسيم الصورة إلى عدد من البلوكات المتداخلة، ومن ثم تطبيق التحويل DCT على كل بلوك. بعد ذلك يتم إجراء عمليات مقارنة لقيم الDCT بين جميع البلوكات، بهدف البحث عن وجود تطابق أو تشابه كبير بينها. تتم عملية المقارنة هذه من خلال حساب المسافة الإقليدية بين قيم ال DCT للبلوكات وذلك بهدف تحديد درجة التشابه بينها والكشف عن وجود مناطق منسوخة وبالتالي الكشف عن تزوير النسخ. في حال كانت المسافة بينهما أصغر من عتبة معينة يتم اعتبار البلوكين أنهما بلوكات محتملة لوجود تزوير نسخ فيها. ولتأكيد كون هذه البلوكات متشابهة يتم مقارنة هذه البلوكات المشتبه حصول التزوير فيها فإذا كان عدد التطابقات أكبر من 20 تطابق عندها تكون المنطقة مزورة.

هذا الأسلوب مناسب للصور الصغيرة وغير مناسب أبداً للصور الكبيرة، لأن عملية التقسيم إلى بلوكات متداخلة، وحساب الDCT لكل منها، ومن ثم المقارنة بينها على مرحلتين، جميعها عمليات مكلفة حسابياً وتؤدي إلى فشل التطبيق وتوقفه عن العمل في حال كانت الصورة كبيرة أو ذات دقة عالية.

إن هذه الطريقة المطبقة في الدراسة الأصلية تعطي إنذارات خاطئة (False Positive) كثيرة تُظهر وجود تزوير في الصورة في حين أنها صورة أصلية، وذلك في المناطق التي تكون متجانسة تماما أو قريبة جداً من التجانس التام كخلفية الصورة أو مشهد لسماء صافية ويعود السبب في ذلك إلى أن قيم الDCT لها تكون متشابهة إلى حد كبير، لذلك ولحل هذه المشكلة وتحسين أداء الخوارزمية، قمنا تحسين هذا الأسلوب وذلك من خلال إضافة خطوات

للخوارزمية الأساسية تقوم بتحديد نسيج البلوك (Texture)، وذلك من خلال الاعتماد على أحد المقاييس التي تقيس نسيج الصورة وهو الإنتروبي (Entropy). لذلك وكخطوة إضافية تهدف إلى التحقق من المناطق المزورة المُكتشفة قبل تأكيد اعتبارها مناطق منسوخة، يتم حساب قيمة الإنتروبي للبلوك المحدد. واعتمادا على قيمة الإنتروبي الناتجة للبلوك إما أن يتم تجاهل البلوك أو يتم اعتباره خاضعاً للتزوير. وقد تم تحديد قيمة هذه العتبة انطلاقاً من أن هذه الإنذارات الخاطئة دائماً تظهر في المناطق المتجانسة تمام أو القريبة جداً من التجانس، لذلك تم تحديد قيمة العتبة ب 1 حيث أن المناطق المتجانسة تماماً تكون قيمة الإنتروبي لها قريبة من الصفر، فإذا كانت القيمة المحسوبة للبلوك أصغر من ال 1 لا يتم أخذه بعين الاعتبار، في حين يُعد البلوك مزوراً عكس ذلك.

وقد تم تحديد هذه القيمة والتحقق من ملاءمتها للنظام المُقترح، والتأكد من التحسين الذي تضيفه على الخوارزمية الأصلية من خلال التجريب على عدد كبير من الصور الأصلية، سنوضح نتائج هذه التجارب لاحقاً، التي تحتوي على خلفيات أو مقاطع متجانسة تقريباً، حيث تبين أن الإنذارات الخاطئة التي كانت تظهر في هذه المناطق قد اختفت تماماً، وفي الوقت نفسه لم تؤثر هذه الإضافة على قدرة النظام في الكشف عن تزوير النسخ. هذه الخطوة المضافة إلى الطريقة الأساسية أدت إلى تحسين كبير في نسبة الإنذارات الخاطئة (False Positive FP).

2.2 الأسلوب الثاني في الكشف عن تزوير النسخ:

يعتمد هذا الأسلوب بشكل أساسي على الدراسة **[6]**. يتم فيه استخدام خوارزمية SURF لاستخلاص النقاط المميزة والمفتاحية (key points) من الصورة واستخلاص سمات وخصائص كل نقطة منها. ثم تتم مقارنة هذه النقاط بالاعتماد على السمات المستخلصة في المرحلة الأولى بهدف البحث عن نقاط متطابقة أو متشابهة إلى حد كبير، مما يدل على وجود منطقة منسوخة عن منطقة أخرى من الصورة وبالتالي يتم الكشف عن وجود تزوير النسخ في الصورة الرقمية.

في المرحلة الثانية التي يتم فيها البحث عن التشابه يتم الاعتماد على بناء شجرة بحث ثنائية KD-Tree، ومن ثم يبحث عن أقرب نقطة أو أقرب مشابه لكل نقطة من النقاط المفتاحية. يتم بعدها حساب المسافة بين كل نقطة وأقرب شبيه (جار) لها، ويتم اعتبارهما متشابهتين إذا كانت المسافة أصغر من عتبة التشابه والتي تكون في هذه الخوارزمية محددة وثابتة لكل الصور، وهذا التشابه يكون دليلاً على وجود تزوير النسخ في الصورة وذلك في المناطق المحيطة بالنقاط المفتاحية المتشابهة.

هذا الأسلوب مناسب للصور الكبيرة الحجم والتي تكون ذات دقة عالية وذلك لأن النقاط المفتاحية المستخلصة من خلال خوارزمية SURF يكون عددها كبيراً وقابلاً للمقارنة بشكل فعال بهدف الكشف عن التزوير، في حين أنها غير مناسبة أبداً للصور الصغيرة ولا تستطيع كشف وجود التشابه في الصورة وذلك لأن عدد النقاط المفتاحية يكون قليلاً جداً وغير كافٍ لتحديد وجود تزوير في الصورة.

وقد تبين من خلال دراسة وتحليل هذه الطريقة المطبقة في الدراسة الأصلية، ومن خلال تجربة تنفيذها على أنماط وأنواع مختلفة من الصور الكبيرة الحجم، أنها تعطي إنذارات خاطئة (False Positive) كثيرة تُظهر وجود تزوير في الصورة في حين أنها صورة أصلية، وقد تبين من خلال الدراسة والبحث أن السبب في ذلك يعود إلى قيمة العتبة الثابتة المفروضة في الدراسة الأصلية ($T_h = 0.045$). لذلك وبهدف تحسين أداء هذه الخوارزمية وللتقليل من عدد الإنذارات الخاطئة قمنا في هذا الأسلوب بتحديد قيمة ديناميكية لعتبة التشابه (وليس قيمة ثابتة كما في الخوارزمية الأصلية)، تختلف قيمة هذه العتبة حسب طبيعة الصورة وعدد النقاط المميزة المستخلصة منها. تم تحديد قيمة عتبة التشابه الديناميكية من خلال التجريب على عدد كبير من الصور واستنتاج العتبة المناسبة لكل صورة، حيث تتغير قيمة هذه

العتبة حسب حجم الصورة وعدد النقاط المفتاحية المستخلصة والتي تتعلق بدورها بطبيعة الصورة. لذلك قمنا بتقسيم الصور إلى ثلاث شرائح، وفي كل شريحة قمنا تحديد قيمة العتبة المناسبة (0.015 و 0.01 و 0.0099).

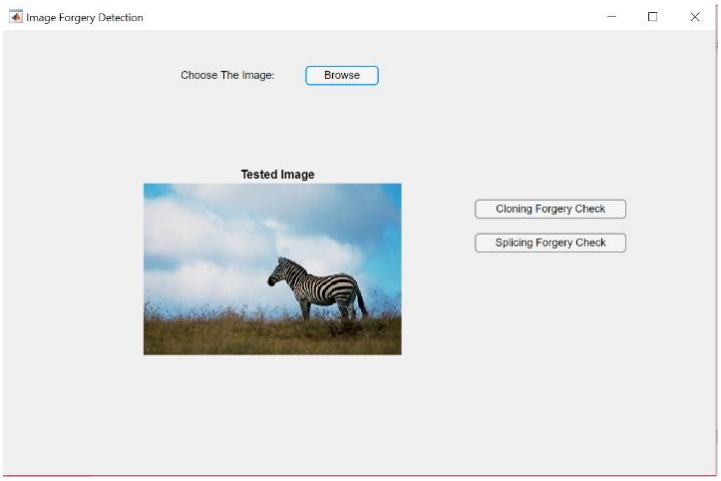
وقد تم تحديد قيمة العتبة الملائمة لكل صورة بالاعتماد على عدد النقاط المستخلصة من الصورة بشكل أساسي، حيث أن العلاقة هي علاقة تناسب عكسي بين قيمة العتبة وعدد النقاط، لذلك يتم إعطاء قيمة أصغر للعتبة كلما كان عدد النقاط المستخلصة أكبر. هذه الإضافة التي قمنا بها كتحسين على الدراسة الأصلية أدت بشكل واضح إلى التقليل من عدد الإنذارات الخاطئة في أماكن غير مزورة في الصورة.

النتائج والمناقشة:

تم تنفيذ هذا التطبيق باستخدام برنامج MATLAB R2019a من خلال استخدام الواجهات والمكتبات التي يوفرها هذا البرنامج، وذلك بسبب ملاءمة هذا البرنامج وقوة أدائه خصوصاً فيما يتعلق بمعالجة وتحليل الصور. حيث تم استخدام البيئة التي توفر إمكانية إنشاء التطبيقات التي تحوي واجهات للمستخدم وذلك من خلال MATLAB App Designer.

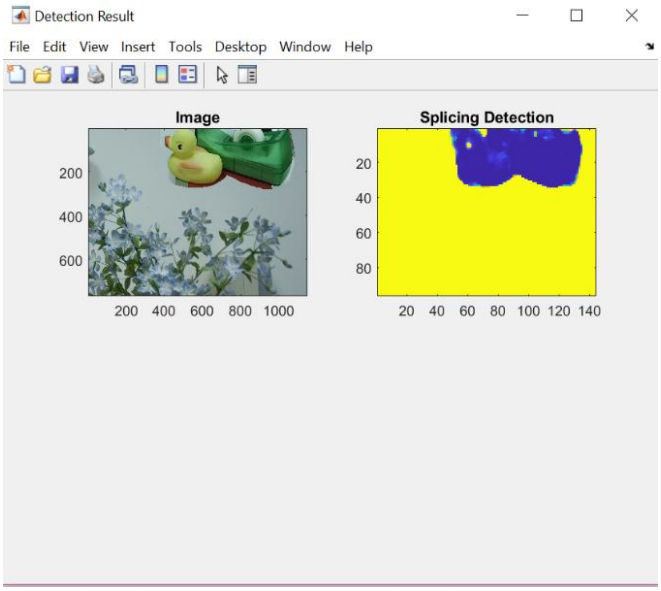
ولاختبار نتائج هذا التطبيق وإمكانية مقارنتها بالدراسات السابقة تم استخدام قاعدتي بيانات للصور هما: CASIA1 **[11]**، و Columbia **[12]**، المستخدمتان على نطاق واسع في الدراسات والأبحاث المتعلقة بالصور، بالإضافة إلى 50 صورة كبيرة الحجم والتي قمنا بتحميلها، ومن ثم تعديلها ليتشكل لدينا 50 صورة إضافية مزورة بالنسخ.

يبين الشكل (2) الواجهة الرئيسية للتطبيق بعد أن تم اختيار صورة من قبل مستخدم النظام وتم تحميلها وعرضها ضمن التطبيق. حيث يستطيع بعدها المستخدم اختيار نوع التزوير الذي يريد التحقق منه.



الشكل (2): الواجهة الرئيسية للتطبيق

في حال كون الصورة أصلية غير مزورة تظهر رسالة للمستخدم توضح خلوّ الصورة من أي تزوير. أما في حال كانت الصورة المطلوب اختبارها مزورة فإن النتيجة تظهر كما هو مبين في الشكل (3)، حيث تظهر الصورة المطلوبة وبجانبها نتيجة الكشف عن تزوير الدمج، ويشير اللونان المختلفان (الأزرق والأصفر) إلى كون الصورة مأخوذة من صورتين مختلفتين تم الدمج بينهما بهدف تشكيل صورة مزورة، لذلك نلاحظ أنه تم الكشف عن وجود تزوير دمج في الصورة بالإضافة إلى تحديد موقع التزوير الحاصل وإظهاره بطريقة تبين للمستخدم مكان الدمج المطبق على الصورة.

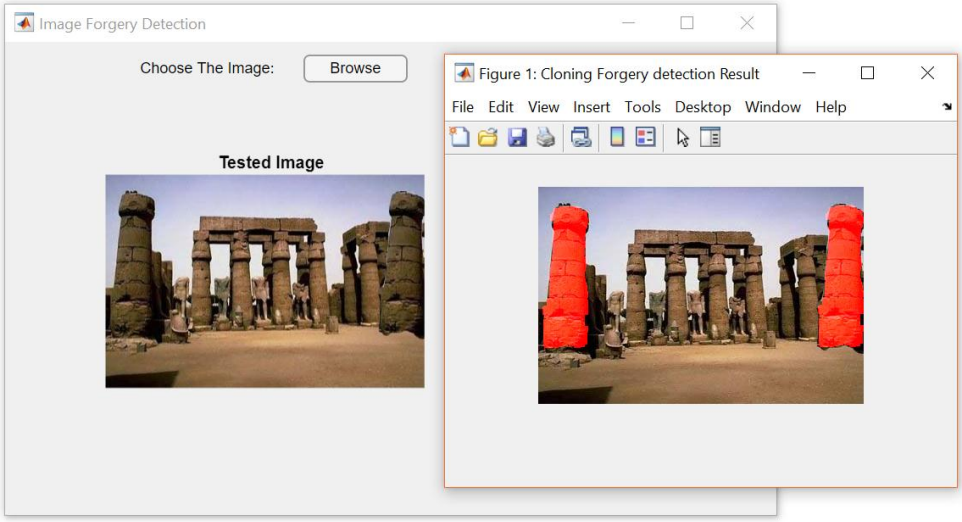


الشكل (3): نتيجة الكشف عن تزوير الدمج في النظام المقترح

أما بالنسبة لتزوير النسخ الذي يتم فيه نسخ جزء من نفس الصورة في موقع آخر منها، فإن التطبيق يختار تلقائياً وبشكل ديناميكي متكيف واحد من الأسلوبين المتبعين في التطبيق وذلك حسب ما يلائم ويناسب الصورة المطلوب دراستها والتحقق منها. سوف نستعرض فيما يلي مثالاً على كل أسلوب وذلك بهدف توضيح النتائج التي تم التوصل إليها، حيث تم تمييز الأسلوب الذي يقوم التطبيق باختياره للكشف عن تزوير النسخ بما يلائم الصورة المدروسة، من خلال لون العلامات التي تدل على مواقع حدوث النسخ، فقد تم اعتماد اللون الأحمر لتحديد البلوكات المنسوخة وذلك للدلالة على أن الأسلوب الأول قد تم تطبيقه، في حين استخدمنا اللون الأخضر للإشارة إلى النقاط المفتاحية المتطابقة للدلالة على استخدام الأسلوب الثاني من قبل التطبيق للكشف عن المواقع المنسوخة.

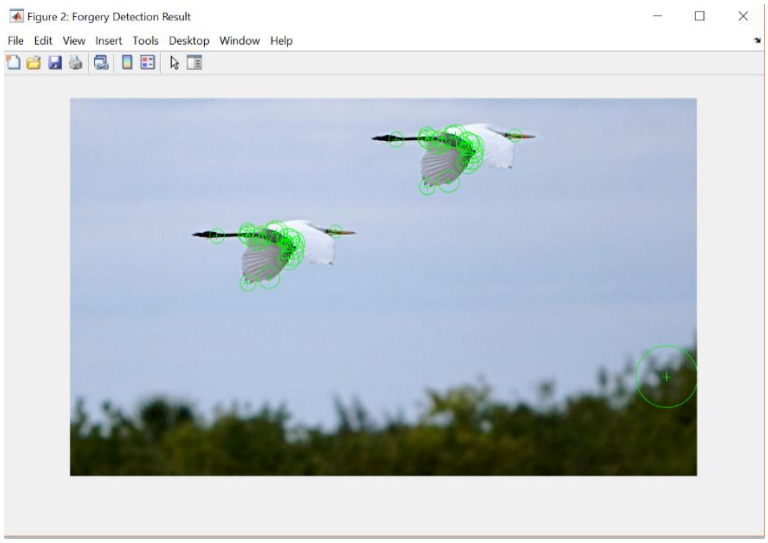
بالنسبة للصور الصغيرة والمنخفضة الدقة والتي لا يزيد حجمها عن (400*400)، يتم تطبيق الأسلوب الأول المعتمد على خوارزمية DCT والمقارنة بين بلوكات الصورة، وتظهر علامات حمراء تشير إلى كل من المنطقة المزورة والمنطقة الأصلية المنسوخة عنها، حيث يتم تمييز هذه البلوكات المتطابقة باللون الأحمر. وقد تم تحديد الحجم المناسب لهذا الأسلوب من خلال تنفيذ التطبيق على صور بأحجام متنوعة، وملاحظة أن النظام يتوقف عن العمل عندما تكون الصورة أكبر من الحجم المناسب.

يبين الشكل (4) الكشف عن تزوير النسخ باستخدام الأسلوب الأول، حيث يظهر على اليسار الصورة المدروسة والتي تم تحميلها إلى التطبيق، في حين يظهر على اليمين نتيجة الكشف عن تزوير النسخ:



الشكل (4): نتيجة الكشف عن تزوير النسخ في الأسلوب الأول

أما بالنسبة للصور الكبيرة الحجم فإننا لا نستطيع تطبيق الأسلوب السابق، حيث يحتاج إلى عدد كبير من المقارنات المكلفة حسابياً إذا كان حجم الصورة كبيراً. لذلك يقوم التطبيق تلقائياً باستخدام الأسلوب الثاني المعتمد على خوارزمية SURF والبحث عن أقرب جار للنقاط، حيث يتم تحديد درجة التشابه باستخدام عتبة ديناميكية يتم تحديدها من خلال التطبيق بحسب الصورة المدروسة، وتظهر علامات خضراء تدل على النقاط المفتاحية المتطابقة والتي تدل على وجود منطقة منسوخة من الصورة في جزء آخر منها كما يبين الشكل (5).

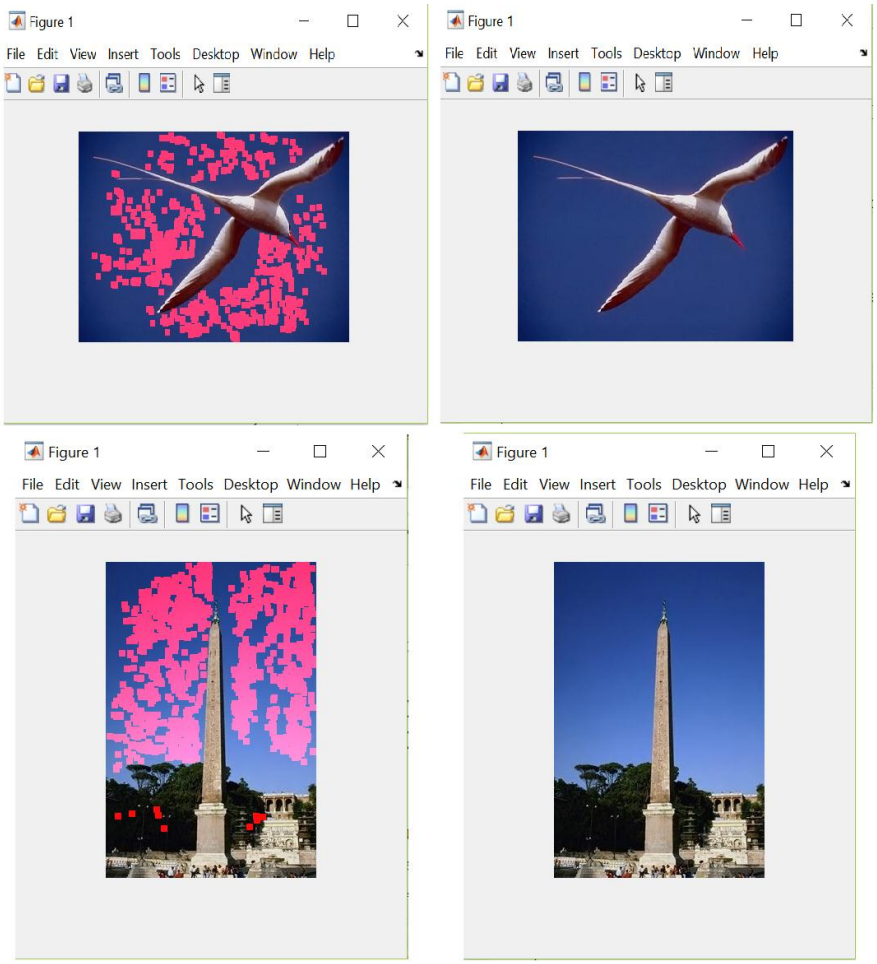


الشكل (5): نتيجة الكشف عن تزوير النسخ في الأسلوب الثاني

تمت الإشارة سابقاً إلى أن هذا التطبيق المُقدم من خلال هذا البحث، إلى جانب الديناميكية التي يقدمها في التكيف مع الصورة المدروسة من خلال اختيار الأسلوب المناسب للكشف عن تزوير النسخ بحسب ما يناسب كل صورة، فهو يقدم أيضاً تحسيناً على كل من الأسلوبين الأساسيين الأول والثاني المتبعين في الكشف عن تزوير النسخ.

ففي الأسلوب الأول المتعلق بالصورة الصغيرة كانت الطريقة الأساسية تُظهر إنذارات خاطئة كثيرة في المناطق المتجانسة إلى حد كبير، وذلك بسبب تشابه السمات والخصائص المستخلصة لهذه البلوكات المتجانسة إلى حد كبير. لذلك قمنا وبهدف التخلص من نقطة الضعف هذه باختبار قيمة الإنتروبي كما هو موضح ومشروح سابقاً.

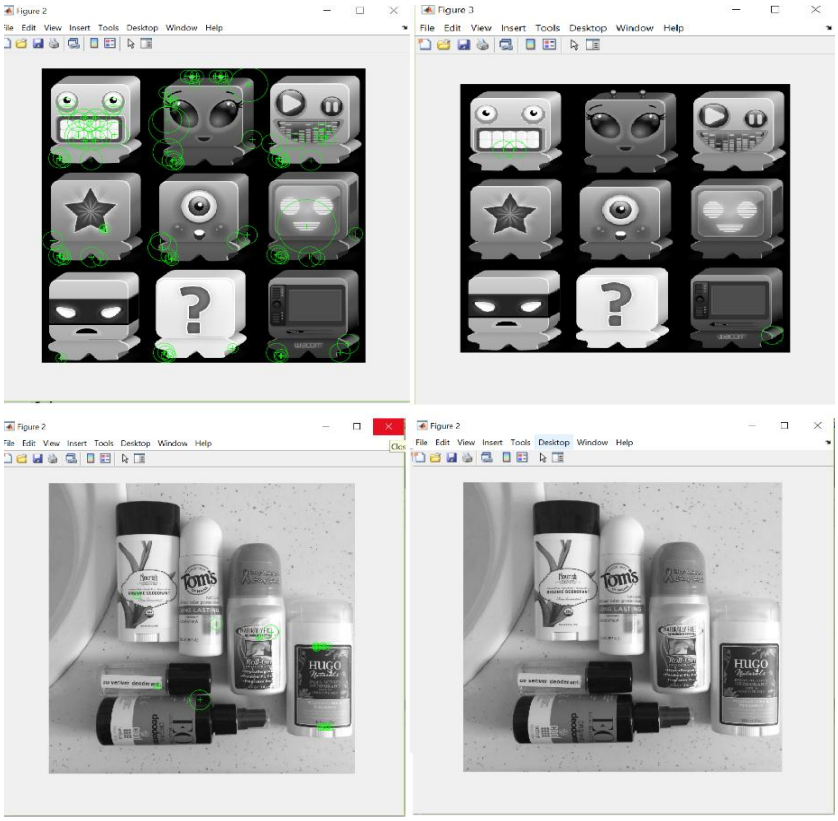
توضح الصور التالية الموضحة في الشكل (6) هذا التحسين حيث تمثل الصور الموجودة على اليسار نتائج تطبيق الخوارزمية الأصلية، في حين تبين الصور على اليمين نتائج الكشف عن تزوير النسخ بعد إضافة الخطوات المُحسنة للخوارزمية:



الشكل (6): التحسين المقدم من خلال النظام المقترح على عدد الإنذارات الخاطئة في الأسلوب الأول

نلاحظ في جميع الصور السابقة أن الخوارزمية الأصلية ينتج عنها عدد كبير من الإنذارات الخاطئة تظهر في الأماكن القريبة جداً من التجانس موضحة من خلال البلوكات الملونة بالأحمر، هذه الإنذارات دلت على وجود تزوير كبير في الصورة في حين أن جميع هذه الصور هي صور أصلية غير مزورة. أما في التطبيق المُقترح ومن خلال الإضافة التي قدمها، فقد تم التخلص من هذه الإنذارات الخاطئة وبالتالي تم تحسين نتيجة الكشف عن التزوير في هذه الخوارزمية، مع الإشارة إلى أن هذا التحسين لم يقلل من أداء الخوارزمية فيما يتعلق بالكشف الصحيح عن وجود التزوير في الصور.

أما بالنسبة للأسلوب الثاني المتبع للكشف عن تزوير النسخ والذي يعتمد على خوارزمية SURF فإن الخوارزمية الأصلية تعاني أيضاً من مشكلة الإنذارات الخاطئة التي تبين وجود التزوير في منطقة أصلية. وقد تم التخلص من هذه الإنذارات أو تقليلها إلى حد كبير من خلال استخدام العتبة الديناميكية بدلاً من العتبة الثابتة كما هو موضح سابقاً. يبين الشكل (7) التحسين الذي قدمه هذا التطبيق على الصور الأصلية الغير مزورة، حيث توضح الصور على اليسار عدد الإنذارات الخاطئة الكبير الناتج عن تطبيق الخوارزمية الأصلية، في حين توضح الصور على اليمين التحسين بعد تطبيق قيمة العتبة الديناميكية حيث قلّ عدد الإنذارات الخاطئة بشكل ملحوظ.



الشكل (7): التحسين المقدم من خلال النظام المقترح على عدد الإنذارات الخاطئة في الأسلوب الثاني

نلاحظ من خلال الشكل السابق التحسين الذي قدمه التطبيق في تقليل عدد الإنذارات الخاطئة، حيث نلاحظ في الصورة الاولى أنه تم خفض عدد الأخطاء من أكثر من 70 خطأ إلى 3 أخطاء فقط، وفي الصورة الثانية من 15 تقريباً إلى 0 أي أنه تم التخلص تماماً من الإنذارات الخاطئة.

إن الأساليب والخوارزميات الأصلية المستخدمة في مجال معالجة الصور وكشف التزوير الحاصل فيها والتي تم الاعتماد عليها في هذا التطبيق، حققت نتائج جيدة ودقة عالية في الكشف عن التزوير، ولكن كانت كل واحدة منها موجهة لنوع أو حجم معين من الصور دون سواه، حيث تقدم نتائج كشف جيدة من أجل هذا النوع المحدد فيما لا تستطيع الكشف عن تزوير أنواع أخرى من الصور أو حتى من الممكن أن تتوقف عن العمل بشكل كامل وتؤدي إلى انهيار النظام. كما أن كل خوارزمية أصلية موجهة فقط لنوع واحد من التزوير دون سواه، وهذا ما يحد من عمل هذه الأنظمة واستخدامها، ففي الدراستين **[6]** و**[7]** يتم الكشف عن تزوير النسخ فقط. في حين أن الدراسة **[10]** تهتم في

الكشف عن التعديلات الحاصلة على الصورة بشكل عام مثل التغبيش وإعادة الضغط أو تغيير الحجم، بالإضافة لكشف التزوير الموضعي الذي يتم على جزء من الصورة كتزوير الدمج. كما لاحظنا أن الأسلوب الأول **[7]** يعمل بشكل جيد من أجل الصور الصغيرة والتي تكون دقتها منخفضة، في حين أن الصور الكبيرة الحجم تسبب انهيار النظام المقترح وتوقفه عن العمل. بينما يستطيع الأسلوب الثاني **[6]** الكشف عن التزوير في الصور الكبيرة والتي تحتوي على عدد كبير من النقاط الهامة بينما يفشل في الكشف عن تزوير الصور الصغيرة.

انطلاقاً من هذه النقاط والملاحظات تم في هذا التطبيق الدمج بين هذه الأساليب وذلك بهدف تقديم إطار عمل أشمل من الأنظمة الموجودة الموجهة للكشف عن التزوير في الصور الرقمية. يوضح الجدول (1) مقارنة بين الأساليب الثلاثة الأساسية (الخوارزميات الأصلية) المُعتمد عليها، وبين النظام المُقترح الخاص بهذا البحث من حيث شمولية التطبيق لأنواع التزوير التي يستطيع الكشف عنها، وحجم الصورة المناسب لكل دراسة وذلك من خلال تجريب صور قاعدة البيانات على هذه الأنظمة:

الجدول (1): مقارنة النظام المقترح بالأنظمة الثلاثة الأساسية

	Splicing Detection	Cloning detection
[7]	NO	Only for small images
[6]	NO	Only for big images
[10]	YES	NO
Our Proposed Method	YES	YES

الهدف الآخر الذي تم العمل عليه في هذا التطبيق هو عدد تخفيض عدد الإنذارات الخاطئة (False Positive) التي كان يعاني منها كل من النظامين الأصليين الموجهين للكشف عن تزوير النسخ. لذلك تم في النظام المقترح معرفة سبب هذه الإنذارات في كل نظام بشكل منفصل، والعمل على سد الثغرات التي يعاني منها، بهدف التخلص نهائياً أو التقليل بنسبة كبيرة من عدد هذه الإنذارات الخاطئة.

بالنسبة للأسلوب الأول في الكشف عن تزوير النسخ للصور الصغيرة **[7]**، فإن المشكلة تكمن في المناطق التي تكون متجانسة بشكل تام أو قريبة جداً من التجانس، فيظهر في هذه المناطق إنذارات وعلامات تبين وجود تزوير فيها على الرغم من كونها أصلية غير مزورة. للمقارنة بين الأسلوب الأساسي والأسلوب المحسن المقدم من خلال هذا البحث، تم اختيار 100 صورة أصلية من قاعدة بيانات الصورة CASIA1 **[11]**. وقد تم اختيار هذه الصور من قاعدة البيانات بحيث تحتوي على مناطق متجانسة تماماً أو قريبة جداً من التجانس، وذلك لأن نقطة الضعف الأساسية في النظام الأصلي تكمن في هذه المناطق. وقد تم تجريب نفس مجموعة الصور هذه والتي يبلغ عددها 100 صورة أصلية على كل من الأسلوبين الأصلي والمقترح وذلك بهدف حساب نسبة التحسين التي قدمتها هذه الدراسة، وقد تبين ظهور عدد كبير من الإنذارات الخاطئة عند تطبيق الأسلوب الأساسي. بينما تمكن النظام المُقترح من التغلب على نقطة الضعف هذه وأدى إلى تقليل عدد الأخطاء بنسبة عالية. يبين الجدول (2) مقارنة بين الأسلوب الأساسي والأسلوب المقترح في هذا البحث، يوضح نسبة الإنذارات العالية التي كان يعاني منها النظام الأصلي في الصور التي تحتوي على خلفيات متجانسة، والنسبة المنخفضة لهذه الإنذارات في النظام المُقترح:

الجدول (2): مقارنة لنسبة الإنذارات الخاطئة في الأسلوب الأول

	False Positive (FP)
[7]	0.74
Our Proposed Method	0.07

أما بالنسبة للأسلوب الثاني المستخدم للكشف عن تزوير النسخ للصور الكبيرة **[6]** فإنه يعاني أيضاً من ظهور عدد من الإنذارات الخاطئة والتي يختلف عددها بحسب الصورة المعطاة. وقد تبين أن هذا العدد يتعلق بحجم الصورة ودقتها، حيث تم الملاحظة أن عدد هذه الإنذارات الخاطئة يزداد كلما كبر حجم الصورة وزادت دقتها. لذلك ومن خلال دراسة وتحليل خطوات عمل هذا النظام تبيَّن أن العتبة الثابتة المفروضة في الدراسة الأصلية غير مجدية وغير متكيفة مع تنوع الصور والأحجام ودرجات الدقة المتنوعة التي تحتاج طبيعة هذا التطبيق إلى وجودها والتكيف والتعامل معها. من هنا تم التوصل إلى ضرورة جعل هذه العتبة ديناميكية متكيفة بحسب الصورة، وليس عتبة ثابتة لجميع الصور. لذلك تم تقسيم الصور إلى ثلاث شرائح بحسب عدد النقاط المميزة المستخلصة والتي تتعلق أساساً بحجم ودقة الصورة، وتم تحديد العتبة لكل شريحة على حدة بحيث نقلل قدر الإمكان من عدد الإنذارات الخاطئة الصادرة عن النظام.

ولحساب نسبة التحسين في عدد الإنذارات الخاطئة، ولأن الدراسة الأساسية لم توضح نسبة الإنذارات الخاطئة، فقد تم تجريب الأسلوب الأساسي والأسلوب المقترح على نفس المجموعة من الصور الكبيرة الحجم. حيث قمنا باستخدام 50 صورة أصلية تم تحميلها من الانترنت. وبعدها تم تعديل هذه الصور باستخدام برنامج تعديل للصور، ليصبح عدد الصور التي تم التجريب عليها 100 صورة، 50 صورة منها هي صور أصلية و50 صورة مزورة بالنسخ. وقد تبين من خلال التجريب على كل من الأسلوب الأساسي المُستخدم في الدراسة الأصلية والأسلوب المُقترح في هذا البحث أن عدد الإنذارات الخاطئة قد قل إلى حد كبير، النسبة موضحة في الجدول، بعد استخدام العتبة الديناميكية التي يقوم التطبيق بتحديدها بما يناسب الصورة في الأسلوب المُقترح، بدلاً من العتبة الثابتة في النظام الأساسي.

وقد تمت عملية المقارنة بين النظامين على مرحلتين: الأولى تم من خلالها حساب عدد الصور التي تظهر فيها إنذارات خاطئة في حين أنها صور أصلية غير مزورة في كل من الأسلوبين، الأساسي والمُقترح، وذلك بهدف تقديم نسبة مئوية للإنذارات الخاطئة في كل منهما. كما هو موضح في الجدول (3) الذي يبين نسبة الإنذارات الخاطئة في كل أسلوب ويُظهر التحسين الذي حققه النظام المُقترح حيث قلت نسبة الإنذارات الخاطئة بشكل كبير.

الجدول (3): مقارنة لنسبة الإنذارات الخاطئة في الأسلوب الثاني

	False Positive (FP)
[6]	0.42
Our Proposed Method	0.06

وفي المرحلة الثانية من المقارنة تم حساب عدد الأخطاء التي تظهر عند الكشف عن تزوير النسخ. حيث أنه تظهر العلامات التي تبين مناطق التزوير، بالإضافة إلى بعض العلامات المتفرقة والتي تظهر في نقاط غير مزورة من الصورة. وقد تم التجريب على كل من النظام الأصلي والنظام المُحسَّن المُقترح، وحساب عدد النقاط المتفرقة الخاطئة التي تصدر عن كل منهما. وقد تبين أنه تم تقليل عدد الإنذارات الخاطئة من 2300 نقطة خاطئة تقريباً في النظام

الأساسي، ليصل العدد إلى 400 نقطة خاطئة في النظام المُقترح، أي أن نسبة التحسين في عدد النقاط الخاطئة عند الكشف عن تزوير النسخ يعادل تقريباً 83%.

الاستنتاجات والتوصيات:

إن الدراسة المقدمة من خلال هذا البحث تهتم بالكشف عن تزوير الصور الرقمية، وموجه بشكل خاص للكشف عن النوعين الأكثر استخداماً من أنواع التزوير وهما تزوير الدمج وتزوير النسخ. حيث تبين أن الأنظمة الموجودة غالباً ما تكون موجهة فقط لنوع معين من التزوير دون سواه، أو أنها لا تعمل إلا في شروط معينة، أو حتى أن بعضها يقدم نتائج جيدة لبعض الأنواع أو الأحجام من الصور، في حين لا يستطيع الكشف عن التزوير في أنواع أخرى، وفي بعض الحالات قد ينهار النظام عندما تكون خصائص ومعطيات الصورة غير ملائمة لطبيعة النظام.

من هنا كان الهدف الأول لهذا البحث هو القدرة على تحقيق نظام يستطيع أولاً الكشف عن أكثر من نوع من التزوير، ويكون قادراً على التعامل مع الصور المختلفة الخصائص بحيث يختار الطريقة الأفضل والأكثر ملائمةً لكل صورة، لتقديم أفضل النتائج في الكشف عن التزوير.

حقق النظام المقترح تحسينا فيما يتعلق بعدد الإنذارات الخاطئة التي كانت تصدر عن الأنظمة الأساسية التي يعتمد عليها التطبيق في الكشف عن تزوير النسخ، حيث أن النظامين الأساسيين المُقدمين في دراسات سابقة كانا يعانيان من عدد كبير من الإنذارات الخاطئة والتي كانت تُظهر وجود تزوير في حين أن الصورة أصلية غير مزورة.

تبين من خلال تحليل هذه الأنظمة أن سبب هذه الإنذارات الخاطئة يختلف بين الدراستين، لذلك تم من خلال هذا التطبيق العمل على حل مشكلة كل طريقة على حدة، وذلك بحل السبب الذي يؤدي إلى ظهور هذه الإنذارات الخاطئة في كل نظام بحسب طريقة عمله.

التطبيق المُقدم من خلال هذا البحث من الممكن الاستفادة منه وتطبيقه في جميع المجالات التي تعتمد في منظومة عملها على الصور، وذلك بهدف التحقق من مصداقية الصورة وأصالتها، تلافياً للأخطاء التي يمكن حدوثها عند استخدام بيانات من صورة قد تكون خاطئة ولا سيما في المجالات الحرجة كالتشخيصات المرضية، والمجال الطبي عموماً، والتحقيقات الجنائية، وكشف الاحتيال وغيرها من المجالات. حيث يقدم هذا التطبيق منظومة عمل تستطيع التعامل مع الصور المختلفة بغض النظر عن طبيعتها أو خصائصها بهدف تقديم نتيجة تكشف عن وجود تزوير في الصورة أو تبين أن الصورة أصلية وموثوقة.

التطبيق المقترح في هذه الدراسة من الممكن تطويره مستقبلاً والعمل على تحسين أدائه بإضافة بعض السمات التي تزيد من قوته. أحد النقاط التي يمكن أن يتم العمل عليها مستقبلاً تتعلق بزمن تنفيذ التطبيق، حيث أنه يحتاج إلى زمن كبير إلى حد ما عندما تكون الصورة كبيرة الحجم أو عالية الدقة. فمن الممكن في بعض الحالات أن يحتاج الكشف عن تزوير صورة كبيرة إلى بضع دقائق، لذلك من الممكن التوجه إلى البحث عن طريقة تخفض كلفة تنفيذ التطبيق وتعمل على تقليل تعقيد الخوارزميات المستخدمة فيه، بهدف زيادة سرعة الأداء، وتقليل الزمن اللازم للكشف عن التزوير. وهذا الأمر هام خصوصاً عند استخدام هذا التطبيق في نظم الزمن الحقيقي كالمنظومات الطبية الافتراضية، على سبيل المثال لا الحصر، والتي تُعد سرعة التنفيذ أحد الركائز الأساسية فيه.

كما يمكن أن يتم العمل على الأسلوب المقترح للكشف عن تزوير النسخ للصور الصغيرة، حيث أنه لا يستطيع الكشف عن المناطق المزورة إذا تم تغيير حجمها أو اتجاهها قبل إعادة لصقها في موقع آخر من الصورة نفسها.

كما أنه من الممكن أن يتم العمل على إضافة ميزة للنظام بحيث تمكن المستخدم من البحث عن الصورة الأصلية، أو الصور التي تم دمجها لتكوين صورة مزيفة، وذلك لمعرفة سبب التزوير الحاصل وإمكانية الحصول على المعلومة الصحيحة، من خلال استخدام نظم استرجاع الصور (Image Retrieval).

References:

[1] Wu, X.; Fang, Z. *Image Splicing Detection Using Illuminant Color Inconsistency*. Third International Conference on Multimedia Information Networking and Security, 2011.

[2] THAKUR, T.; SINGH, K. R.; YADAV, A. *Blind Approach for Digital Image Forgery Detection*. International Journal of Computer Application, 2018.

[3] GULIVIDALA, S.; RAO, C. S. *RST Invariant Image Forgery Detection*. Indian Journal of Science and Technology, 2016.

[4] MANJUSHREE, D.; SURESH, L.; KUMAR, S. *Image Forgery Detection Using Adaptive over Segmentation and Feature Point Matching*. International Journal of Innovative Research in Computer and Communication Engineering,Vol 4, No. 6, 2011.

[5] MUHAMMAD, G.; Al-HAMMADI, M. H.; HUSSAIN, M.; BEBIS, G. *Image forgery detection using steerable pyramid transform and local binary pattern*, 2014.

[6] SHIVAKUMAR, B. ; & BABOO, L. D. *Detection of Region Duplication Forgery in Digital Images Using SURF*. IJCSI International Journal of Computer Science Issues, 8(4), (2011, July).

[7] JADHAV, N.; KHARAT, S.; NANGARE, P. *Copy-Move Forgery Detection Using Dct*. International Journal of Emerging Technologies and Engineering, Vol. 2, No. 3, 2015.

[8] THAKUR, T.; SINGH, K. R.; YADAV, A. *Blind Approach for Digital Image Forgery Detection.* International Journal of Computer Application, 2018.

[9] KASHYAP, A.; GUPTA, H. O. *An Evaluation Of Digital Image Forgery Detection Approach*. International Journal of Applied Research, 2017.

[10] DIRIK, A. E.; MEMON, N. *Image tamper detection based on demosaicing artifacts.* 16th IEEE International Conference on Image Processing (ICIP), 2009, 1497–1500.

[11] *Iris Database*. Retrieved from Center for Biometrics and Security Research, 2019. <http://www.cbsr.ia.ac.cn/irisdatabase/download/version1/CASIA1.rar>

[12] *Columbia Uncompressed Image Splicing Detection Evaluation Dataset*, 2019. <http://www.ee.columbia.edu/ln/dvmm/downloads/authsplcuncmp/>