الخلاصة

بات التطورذلك،ئل في استخدام الإنترنت كرسائل البريد الإلكتروني ومواقع التواصل الاجتماعي مثل Facebook و Twitter و Instagram، مادة مهمة للباحثين سواء في تحقيق أهدافهم في مختلف ميادين المعرفة، ومن بينها أمن المعلومات. اذ استخدمت العديد من الأساليب مثل التشفير واخفاء المعلومات لنقل البيانات بأمان إلى المستفيدين دون أي تعديلات، الا ان اغلب تلك الخوارزميات تفتقد إلى مراحل المعالجة المسبقة.

هناك عدد قليل من خوارزمية إخفاء المعلومات التي تتضمن مراحل معالجة أولية لكل من الرسائل السرية ومقاطع فيديو الغلاف. علاوة على ذلك ، تعاني تلك التقنيات من ضعف كبير في عدة جوانب ، بما في ذلك الأمن ، والقدرة على التضمين ، وعدم الإدراك ، والقوة ضد الهجمات.

في هذا البحث ، يتم إخفاء أو تضمين الرسالة السرية في إطارات/بكسلات معينة ضن الفيديو الأصلي بشكل عشوائي بواسطة مسجل الإزاحة ذو التغذية المرتدة الخطية بعد ان يتم تشفير الرسالة السرية باستخدام طريقة فيجنير المعروفة، وبذلك يتم زيادة مستوى الأمان الناتج بالمقارنة مع الطريقة التي لا تتضمن تلك الإجراءات المسبقة قبل التضمين. كما ان عملية اختبار وتقييم الطريقة المقترحة تتم باستخدام معيارين هما متوسط الخطأ التربيعي (MSE) وقيمة نسبة الإشارة إلى الضوضاء .(PSNR) ولابد الأول:ارة أيضا الى ان الرسالة المخفية تبقى محمية حتى لو تم اختراق كائن stego لأن المهاجمين بحاجة إلى معرفة مفتاح التشفير المستخدم وأماكن (إطارات/بكسلات) التضمين وبالتالي إعادة بناء الرسالة الاصلية بنجاح .

النتائج التجريبية حققت قدرة تضمين جيدة، وعدم إدراك أفضل لمقاطع الفيديو. علاوة على ذلك ، تزيد مراحل المعالجة المسبقة من أمان ومتانة الطريقة المقترحة عند مقارنتها بطرق إخفاء المعلومات أخرى.