University of Mosul
College of Computer Science
and Mathematics

New Hybrid Technique for Enhancing Data Security

A Thesis Submitted by

Ammar Abdul Majed G. Al-Mashhdani

M.Sc. / Thesis
Computer Science

Supervised by

Dr. Ahmed Sami Nori

Assistant Professor

2021 A.D. **1442 A.H.**

Abstract

The rapid development in hardware and software, made life easy. However, with this development and the ease presented by it, it is necessary to mention the concerns or the negatives that must be taken into account, which is the security of data and information, that has become a big problem and an obstacle to this development. It is necessary to improve and devise new methods to repel these attacks or delude attackers with new methods, and the most famous of these attacks is the brute force attack, which poses a great danger to most data encryption algorithms.

Since the approach of data security are divided into two main parts, cryptography and steganography, a new method has been proposed that adopts the integration of cryptography and steganography to take benefit of their advantages to improve security and to repel brute force attack and some attacks on them, effectively when sending an image containing confidential information. Thus, the first step is to encrypt the message using the ElGamal algorithm, which is one of the public-key encryption methods. The creation of keys in this algorithm is by applying special laws to be valid in ElGamal encryption, which means achieving security and authentication.

As for the second step, the message password will be encrypted with the Honey encryption algorithm, which produces a valid text of appearance and meaning, but fake work and use. Thus, it works to create N honey passwords from the real password entered by the user to deceive the attacker in choosing the correct word among the honey words, then encrypt honey words with the hash function, salting and storing them in special tables that are ways to defend the (dictionary, rainbow) attacks and then apply the XOR function.

The third step is to collect the data with all the variables for each of the ElGamal algorithm and the Honey algorithm and hide them inside the

image in a random Least Signified Bit (LSB) method by using the three colors Red-Green-Blue (RGB) and through the public key that is known to the sender and recipient and by applying the XOR function when hiding the data in the image.

Based on a computer model with specifications (Windows10-based, processor (2.53 GHz), with 8 Gigabyte RAM) and after the application and measurement of the results achieved, it show the efficiency of the proposed system in terms of achieving data security and resistance to some types of attacks and reveal the evaluation criteria that showed the proposed system good performance, as it achieved high performance and accuracy as in the Peak Signal-To-Noise Ratio (PSNR) scale up to 89 (dB) and in the Mean Square Error (MSE) scale up to 0.00128

In the Structural Similarity Index Measurement (SSIM) scale up to 0.9999999 (between two images before and after embed) and in the correlation coefficients between its adjacent pixels, scale up to 0.0001(stego-image, original image).

جـــامعـــة الموصـــل
كلية علـوم الحاسـوب
والرياضيات

تقنية هجينية جديدة لتحسين أمن البيانات

عمار عبد المجيد غربي المشهداني

رسـالـة ماجسـتير
علـوم الحاسـوب

بإشراف
د. أحمد سامي نوري
أستاذ مساعد

١٤٤٢ هـ ٢٠٢١ م

المستخلص

التطور السريع في الأجهزة والبرمجيات جعل الحياة سهلة. لكن مع هذا التطور والسهولة التي يقدمها، لا بد من ذكر المخاوف أو السلبيات التي يجب مراعاتها، وهي أمن البيانات والمعلومات، والتي أصبحت مشكلة كبيرة وعقبة أمام هذا التطور. من الضروري تحسين وابتكار أساليب جديدة لصد هذه الهجمات أو توهم المهاجمين بأساليب جديدة، وأشهر هذه الهجمات هو هجوم القوة الغاشمة الذي يشكل خطراً كبيراً على معظم خوارزميات تشفير البيانات.

نظرًا لأن نهج أمان البيانات ينقسم إلى جزأين رئيسيين، التشفير وإخفاء المعلومات، فقد تم اقتراح طريقة جديدة تعتمد دمج التشفير وإخفاء المعلومات للاستفادة من مزاياها لتحسين الأمان وصد هجمات brute force وبعض الهجمات الأخرى، بشكل فعال عند إرسال صورة تحتوي على معلومات سرية. وبالتالي، فإن الخطوة الأولى هي تشفير الرسالة باستخدام خوارزمية ElGamal، وهي إحدى طرق تشفير المفتاح العام. يتم إنشاء المفاتيح في هذه الخوارزمية من خلال تطبيق قوانين خاصة لتكون صالحة في تشفيرElGamal، مما يعني تحقيق الأمان والمصادقة.

أما بالنسبة للخطوة الثانية، فسيتم تشفير كلمة مرور الرسالة باستخدام خوارزمية تشفير Honey، والتي تنتج نصًا صالحًا للمظهر والمعنى، ولكن العمل والاستخدام مزيفين. وبالتالي، فإنه يعمل على إنشاء N من كلمات مرور معسولة (Honeyword) من كلمة المرور الحقيقية التي أدخلها المستخدم لخداع المهاجم في اختيار الكلمة الصحيحة من بين Honeyword ، ثم تشفير Honeyword بدالة Hash وأضافة لها Salting وتخزينها في جداول خاصة هي طرق. للدفاع عن هجمات (Dictionary، Rainbow) ثم تطبيق دالة XOR.

الخطوة الثالثة يتم جمع البيانات وكافة المتغيرات لكل من خوارزمية ElGamal وخوارزمية Honey واخفاءها بداخل الصورة بطريقة LSB العشوائية واستخدام الألوان الثلاثة RGB وعن طريق المفتاح العام الذي يكون معلوماً لدى المرسل والمستلم وبتطبيق دالة XORعند اخفاء البيانات بالصورة.

اعتمادا على نموذج حاسوبي بمواصفات Windows10-based, processor 2.53 with 8 Gigabyte RAM،GHz)) وبعد التطبيق وقياس النتائج المتحققة تبين لنا كفاءة النظام المقترح من حيث تحقيق امن البيانات ومقاوم لبعض أنواع من الهجمات وتكشف مقاييس التقييم التي أظهرت النظام المقترحة أداءً جيدًا، حيث حققت أداء ودقة عالية كما في مقياس PSNR يصل الى (89 dB وفي مقياس MSE يصل الى 0.00128

في مقياس Structural Similarity Index Measurement (SSIM) يصل إلى ٠,٩٩٩٩٩٩٩ (بين صورتين قبل وبعد التضمين) وفي Correlation Coefficients بين وحدات البيكسل المجاورة يصل مقياسها إلى ٠,٠٠٠١ (صورة stego، الصورة الأصلية).