بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

: قال الله تعالى

وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ۖ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ
الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ ﴿١٠٥﴾

صدق الله العظيم
سورة التوبه

ACKNOWLEDGEMENTS

I would like to praise God for his unscathed donation of belief and empowerment upon myself not only in course of this work towards my Bachelor degree but throughout my entire life.

My deepest gratitude goes first and foremost to my supervisor ***Dr.IBRAHIM KHIDER ELTAHIR***, for his constant support and guidance, patience during the whole period of this research.

Secondly I would like to express my greatest gratitude to my beloved teacher Rasha jalal for her guidance and to my beloved colleague Eng.Azza Kamal for her help during the implementation of the software.

Great appreciation goes to my Brother and my friend Ismail Najmuldin for his constant support.

To my friends and those who their name slipped and not mentioned thank you for your support and your encouragement.

I should mention that without my beloved family I would not even be where I am now. I am very blessed to have such family and thank them with all my heart for their prayer, encouragement and their time gave to me to do this study.

مستـــخلـص

هذا البحث يتناول توضيح لطرق أمن المعلومات القديم منها والحديث حيث إنه يهدف إلى المحافظه على امن المعلومات النصيه (سريتها ، خصوصيتها) وذالك بتشفيرها

بإستخدام خوارزميه إلالتفاف ،خوارزمية الوصول العشوائي ، خوارزمية البت الإقل أهميه أساس الوصول العشوائي وخوارزمية إلالتفاف اساس الوصول العشوائي ومن ثم إرسال الصوره الى المستقبل ليتم إستخراج النص المشفر وفك شفرته. كما يقارن مدى تأثير هذه الخوارزميات المختلفة على الصوره بحساب متوسط مربع الخطأ و معدل الازعاج الى الاشارة القصوى للصوره ، وأيضا ينا قش مدى العلاقة بين حجم الصوره وحجم المعلومات المراد إخفائها .

تم تمثيل نظام للإخفاء باستخدام لغه ماتلاب حيث يسمح للمستخدم بإختيار الصوره وتحديد خوارزميه الإخفاء ومن ثم إدخال المعلومات كتابتآ إذا كانت رساله قصيره أوإدخال المسار إذا كانت محفوظه بملف داخل الجهاز .

تم الحصول على النتائج ومنا قشتها و قد تبين أن تأثير خوارزمية الوصول العشوائي على الصوره يكون مرئي في شكل نقاط سوداء بينما خوارزمية البت الإقل أهميه وخوارزمية الإلتفاف ليس لهما تأثير مرئي لانهما يعملان علي تغير البت الإقل أهميه وإستجابه العين لاتستطيع إن تدرك هذ التغير.أيضا أظهرت النتائج إن خوارزمية البت الإقل أهميه أساس الوصول العشوائي وخوارزمية الإلتفاف أساس الوصول العشوائي هما الأفضل اذا ان من خلالهما يتم الوصول لعناصر الصوره بطريقه عشوائيه وذالك يوفر التثبيت العشوائي للمعلومات فالايستطيع أحد معرفة ترتيبها غير المرسل وهذا يضيف مستوى آخرمن السرية للمعلومات.

وبذلك نخلص الى انه لايوجد تأثير مرئي على الصوره اذا كان معدل الزعاج الى الاشارة القصوى اكبر من 40 ديسيبل وحجم المعلومات صغير قارنه بحجم الصوره.

ABSTRACKT

This dissertation is a description of the information security techniques and in the first place, it aimed to maintain the information security (privacy, Confidentiality) by encrypting it using RSA algorithm and hid it into image

spatial domain using different algorithms like Least Significant Bit algorithm ,Convolution or Bit XOR algorithm , Random approach algorithm ,Least Significant Bit based Random approach algorithm and Convolution based Random approach algorithm and hence transmits the image to the Receiver to Extract the information and decrypt it. Also it compares the effect of these algorithms on the image by calculating Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). And also it explains the relation between information Size and image size.

By using MATLAB language the Steganography system was implemented and it allow user to select an image and determine the Steganography algorithm and hence enter the information which it can be short message or file.

The results were obtained and discussed and it shows that the Random approach algorithms have visible impact on the image appears as black spot while Convolution algorithm or Least Significant Bit algorithm does not have A visible impact on the image because the precision in many image formats is far greater than that perceivable by average human vision. Also the results shows that the Least Significant Bit based Random approach algorithm and Convolution Based Random approach algorithm are the best because the information are embed randomly so no one except the receiver Know the order of the information in side

image and this add Another level of security to the information.

And it concludes that there are no visible impacts on the image when the PSNR is greater than 40dB and the information size is small compared to the image size.

Contents

List of Tables

Tables Description **Page Number**

List of Figures

List of Abréviations

AES	Advance encryption standard
DES	Data Encryption Standard.
GUI	Graphical User Interface
GIF	Graphics interchange file
LSB	Least Significant Bit
MATLAB	MATrix LABoratory
MSE	Mean Square Error
Pixel	Picture element
PKC	Public Key Cryptography.
PSNR	Peak Signal to Noise Ratio
RSA	Ronald Rivest Adi Shamir Leonard Adleman
SKC	Secret Key Cryptography.
TCP/IP	Transmission Control Protocol /Internet Protocol
XOR	Exclusive OR