

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

قَالَ اللَّهُ تَعَالَى:

﴿تَرْفَعُ دَرَجَاتٍ مَن نَّشَاءُ ۖ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ﴾

الآية ﴿٧٦﴾ سورة يوسف

صدق الله العظيم

Dedication

*To my parents for their love and support
throughout my life.....*

To my beloved brothers and sisters....

*To my Teachers, Students, Friends and everyone
who have been a part of my life.....*

ACKNOWLEDGEMENT

First, I would like to thank Allah for giving me the power and health to do this work.

*Second, I would like to express my special thanks to my supervisor **Dr: Faísal Mohammed Abdallah** for the guidance, encouragement and advice.*

I am indebted to the Sudan University of Science & Technology for providing the facilities to conduct this work.

Finally, grateful acknowledgement is made to all those who participated with their time, effort, advise and knowledge to make this a successful study.

ABSTRACT

The increase use of the electronic communication demands more security on the exchange of the critical information. cryptography now a day's get more and more important to address this issue. encryption algorithms available for textual data are highly efficient. but sometime the information is available in form of image. in such cases we need a specialized algorithm that is highly optimized to protect pictorial information. in this research two state tables are used to solve correlation problem between the public known output of internal state by using permutation between state1 and state2 that is improve the RC4 algorithm. the enhanced RC4 Algorithm is used for images encryption and decryption the results obtained show that, the enhanced RC4 achieved high security compared with standard RC4, so it can be used in WEP protocol instead of RC4 to overcome weak keys problem. diehard statistical test tool is used to test the randomness of the enhanced RC4 algorithm, also we measure the efficiency of the method using Peak Signal -to-Noise Ratio (PSNR)and mean squared error (MSE) and results obtained give optimum values of robustness.

المستخلص

إن التطور السريع في المجالات التقنية أدى إلى زيادة الإتصال الإلكتروني مما يتطلب تحسين التأمين لتبادل المعلومات الحساسة . يعتبر علم التشفير من العلوم المهمة بتلك القضايا . خوارزميات التشفير المستخدمة للبيانات النصية ذات كفاءة عالية ، ولكن في بعض الأحيان المعلومات تكون في شكل صور وبالتالي نحتاج إلى خوارزميات متخصصة لحماية معلومات الصورة . في هذا البحث قمنا بإستخدام (two state table) لحل مشكلة الارتباط بين الناتج المعروف مسبقاً داخل الـ (state) بإستخدام تبديل بين الـ (state1) و (state2) لتحسين خوارزمية (RC4). الخوارزمية المحسنة تم إستخدامها في تشفير وفك تشفير الصور . وكانت النتيجة الحصول على خوارزمية محسنة حققت درجة عالية من الأمان مقارنة بـ (RC4) ولذلك يمكن إستخدامها في بروتوكول الـ (WEP) بدلاً من الـ (RC4) لتفادي مشكلة ضعف المفاتيح . لقد قمنا بإستخدام أداة (Diehard) الإحصائية لإختبار العشوائية في خوارزمية (RC4) المحسنة ومن ثم قمنا بقياس كفاءة الخوارزمية بإستخدام (PSNR) و (MSE) والقيم الناتجة من الخوارزمية أعطت نتائج جيدة.

List of Tables

Table Name	Page Number
Table 4.1 show the result of MSE and PSNR value.	39
Table 4.2 show the result of images and histogram.	40
Table 4.3 Result of randomness test between enhanced RC4 and standard RC4.	42
Table 4.4 Result of Diehard Tests between enhanced RC4 and standard RC4.	42

List of Figures

Figure Name	Page Number
Figure 2.1 show Symmetric cryptography system	10
Figure2.2 show Asymmetric cryptography system	13
Figure 3.1 Flow chart of basic operation of encryption process by ERC4	28
Figure 3.2 Flow chart of basic operation of encryption process by ERC4	29
Figure 4.1 Flow chart of Image encryption	36
Figure 4.1 Flow chart of Image Decryption	37

List of Abbreviations

Abbreviations	Stand For
RC4	Rivest Cipher
WWW	World Wide Web
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
DES	Data Encryption Standard
AES	Advance encryption Standard
LFSRs	Linear Feedback Shift Registers
KSA	Key Scheduling Algorithm
PRGA	Pseudo Random Generator algorithm
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
ERC4	Enhanced Rivest Cipher

Contents

أية.....	I
Dedication.....	II
Acknowledgment.....	III
Abstract.....	IV
المستخلص.....	VI
Contents.....	VII
List of Tables.....	XI
List of Figures.....	XII
List of Abbreviations.....	XV
Chapter1 : Introduction	1
1.1 Overview.....	1
1.2 Problem statement.....	2
1.3 Research Objectives.....	2
1.4 Methodology	2
1.5 Research scope.....	3
1.6 Thesis out line	4
Chapter 2: Literature Review and Related Work.....	5
2.1 Introduction.....	5
2.1.1 How does cryptography work.....	5
2.2 Classical encryption techniques.....	5
2.2.1 Caesar Cipher	6
2.2.2 Playfair Cipher	6
2.2.3 Poly-alphabetic Cipher	7
2.2.3.1 Vigenère algorithm	7
2.3 Cryptographic systems Classification	8
2.3.1 Symmetric Cryptography.....	9

2.3.1.1 Symmetric Strengths.....	10
2.3.1.2 Symmetric Weaknesses.....	11
2.3.2 Asymmetric Cryptography	11
2.3.2.1 Asymmetric Strengths	14
2.3.2.2 Asymmetric Weaknesses	14
2.3.3 Block cipher	14
2.3.3.1 Data Encryption Standard	15
2.3.3.2 Advanced Encryption Standard.....	15
2.3.3.3 RC2.....	16
2.3.4 Stream cipher	16
2.4 Shift register	17
2.4.1 A5 – Encryption	17
2.4.2 A5/1.....	19
2.5 RC4 Encryption Algorithm.....	19
2.5.1 RC4 Features.....	19
2.5.2 RC4 Strengths	20
2.5.3 RC4 Weakness	20
2.6 Cryptanalysis	21
2.7 Related Studies	22
Chapter3 : PROPOSED METHOD AND TOOLS.....	25
3.1 Overview	25
3.2 Digital Images	25
3.2.1 Type of Digital Images.....	25
3.3 Image Encryption Techniques.....	26
3.4 Proposed Method..	26
3.4.1 Standard RC4 Method	26
3.4 .2 Enhanced RC4 Method..	27

3.4.3 Flow chart of Enhanced RC4 Process.....	27
3.5 Algorithm Performance	30
3.5.1 Mean Square Error	30
3.5.2 Peak signal to Noise ratio	30
3.5.3 Randomness Test.....	31
3.5.4 Random number generation Tests.....	31
3.5.5 The Frequency Test.....	31
3.5.6 Diehard Tests.....	32
3.5.6.1 Runs Tests.....	32
3.5.6.2 Count the 1's in specific bytes Test.....	32
3.5.6.3 Overlapping sums Test	32
Chapter 4: Simulation and Result.....	33
4.1 Simulation Environments.....	33
4.1.1 Java	33
4.1.1.1 Significant Language Features.....	33
4.1.2 MATLAB	34
4.2 Image formats supported by Matlab.....	35
4.3 Flow chart	35
4.4 MSE and PSNR.....	38
4.5 Histogram.....	40
4.6 Randomness Tests.....	42
Chapter 5: Conclusion and Recommendations.....	45
5.1 Conclusion	45
5.2 Recommendations.....	45
References.....	46
Appendixes.....	48