الآيـــــة

بِـــسْـــمِ اللّـــهِ الـــرَّحْـــمـــنِ الـــرَّحِـــيـــمِ

قال تعالى:

﴿اللَّـــهُ لَا إِلَـــهَ إِلَّا هُوَ الْحَيُّ الْقَيُّومُ لَا تَأْخُذُهُ سِنَةٌ وَلَا نَوْمٌ لَّهُ مَا فِي السَّمَاوَاتِ وَمَا فِي الْأَرْضِ مَن ذَا الَّذِي يَشْفَعُ عِندَهُ إِلَّا بِإِذْنِهِ يَعْلَمُ مَا بَيْنَ أَيْدِيهِمْ وَمَا خَلْفَهُمْ وَلَا يُحِيطُونَ بِشَيْءٍ مِّنْ عِلْمِهِ إِلَّا بِمَا شَاءَ وَسِعَ كُرْسِيُّهُ السَّمَاوَاتِ وَالْأَرْضَ وَلَا يَئُودُهُ حِفْظُهُمَا وَهُوَ الْعَلِيُّ الْعَظِيمُ﴾.

صـــدق اللّـــه الـــعظـــيم

سورة البقرة الآية ﴿255﴾

Dedication

Who taught me that achieving the goals with effort and work

not with wishful thinking, who prayed for me

My beloved father.

Who taught me that donation is unconditional, Words are inadequate in offering your prerogative and my thanks

my beloved mother.

Who supported me, supported me and shared with me every moment, who stood beside me to complete this work

my beloved husband.

Who were spent our memorable days and sweet time, to those who am I happier with them

my beloved brothers.

AKCNOWLEDGEMENTS

Words are inadequate in offering my thanks to **ALLAH** for helping me and always reconcile me, praise be to **ALLAH**.

As I wish to express my deep sense of gratitude to my supervisor **Dr. Fisal Mohammed Abdalla,** for his outstanding guidance and support which helped me in completing my thesis work.

Besides my advisors, it is a matter of great privilege for me to present this project to my thesis examiners, for being a part of this work, to collage of computer science and information technology **(CCSIT)** and to Sudan University of Science and Technology **(SUST).**

Last, but not least, I would like to express my heartfelt thanks to my **parents**, my **brothers** and my **husband** for unconditional support and encouragement to pursue my interests, for listening to my complaints and frustrations, and for believing in me I can go ahead to success. To my friends **Sherin** and **Amal** Who spend their time and effort for help my and wishes for the successful completion of this project and to my beloved friend **Sahar Alsiddig** and everyone who was prayer for me.

ABSTRACT

An online payment system is an Internet-based method of processing economic transactions. It allows a vendor to selling and obtains payments over Internet. The main components of online payment system are: customer who asked for a service, merchant who provides a services and bank who transfer a fund between them; to accomplish these processes customers are asked to providing personal details along with additional bank details, the major problem here is the responsibility of protecting customer's information from being misused or being exposed. The thesis provides solution to protecting information of a customer by using cryptographic techniques that restricting who see what and to prevent customer against anti-phishing attack. Some of these techniques like technique based on secret sharing that allow secret to be share among set of participants to make the recovering of a secret from set of shares is difficult, Advanced Encryption Standard (AES) is applied on shares to provide confidentiality and steganography as extra security layer. The main part of the solution that provide privacy and authority to customer's information is the use of certified authority as trusted third party between merchant and customer, it's extracting secret info and send least of customer info as account number to the merchant and secret info like PIN number to the bank. This solution prevent merchant from misused of customer info and if merchant side is a phishing website, it'll not gain any secret info about a customer so that is providing privacy to the customer.

الـــمستخلص

نظام الدفع عبر الإنترنت هو طريقة تعتمد على الإنترنت في معالجة المعاملات الاقتصادية، ويسمح للبائع بإجراء عملية البيع والحصول على المدفوعات عبر الإنترنت .المكونات الرئيسية لنظام الدفع عبر الإنترنت هي: العميل الذي يطلب الخدمة، ومزود الخدمة الذي يقدم الخدمات والبنك الذي يقوم بتحويل الأموال بينهم. لإنجاز هذه العمليات، يُطلب من العملاء تقديم تفاصيل شخصية بالإضافة إلى التفاصيل المصرفية، تكمن المشكلة الرئيسية هنا في مسؤولية حماية معلومات العميل من إساءة استخدامها أو إمكانية حصول الغير واطلاعهم عليها. توفر الأطروحة حلًا لحماية المعلومات عن طريق تحديد صلاحيات الوصول لبيانات العملاء، كما توفر تقنيات تحمي البيانات من الخداع الإلكتروني. بعض من التقنيات المستخدمة تقنية التشفير المعتمدة على المشاركة السرية التي تسمح للمعلومة السرية بالمشاركة بين مجموعة من المشاركين لجعل استرداد المعلومة السرية من جزء من مجموعة من المشاركين أمراً صعباً، كم تم تطبيق خوارزمية التشفير المعياري المتقدم (AES) لتوفير الموثوقية ، وخوارزمية إخفاء المعلومات لتوفير المزيد من السرية وللحماية من هجمات كهجمات التحليل الإحصائي. يتمثل الجزء الرئيسي من الحل الذي يوفر الخصوصية والسلطة للمعلومات في استخدام طرف ثالث موثوق به بين مزود الخدمة والعميل، حيث يقوم هذا الطرف باستخراج معلومات العميل السرية وإرسال أقل معلومات عنه كرقم الحساب إلى مزود الخدمة أما المعلومات السرية مثل رقم التعريف الشخصي (PIN) فيتم إرساله للبنك. يمنع هذا الحل مزود الخدمة من إساءة استخدام معلومات العميل وإذا كان مزود الخدمة هو موقع ويب للتصيد الاحتيالي، فلن يحصل على أي معلومات سرية حول العميل، وهذا يوفر الخصوصية للعميل .

List of Tables

Table No.	Table Name	Page No.
Table 2.1	Naor and Shamir's scheme for encoding to share a Binary image into two shares	25
Table 4.1	Comparison between proposed solution and related works	69

List of Figures

Figure No.	Figure Name	Page No.
Figure 2.1	Cipher model classifications	7
Figure 2.2	Symmetric key cryptosystem	9
Figure 2.3	AES structure	12
Figure 2.4	First round process	12
Figure 2.5	Public key cryptography	15
Figure 2.6	Information hiding classification	16
Figure 2.7	Stenographic operation	17
Figure 2.8	Image steganography	19
Figure 2.9	LSB sampling	19
Figure 2.10	IPv4 Header	20
Figure 2.11	a random column-permutation of white pixel and black pixel is done from S0 and S1	23
Figure 2.12	C0 and C1 are the two column matrices of white and black pixel respectively which is selected on random basis	24
Figure 2.13	Example of Moiré patterns	28

List of Figures

Figure No.	Figure Name	Page No.
Figure 2.14	Generation of Moiré patterns	29
Figure 3.1	System's Block Diagram	33
Figure 3.2	Sequence Diagram for Checkout Process	35
Figure 3.3	Sequence Diagram for Payment Process	36
Figure 3.4	Flowchart for System processes	37
Figure 3.5	Flowchart for payment process	38
Figure 3.6	Flowchart for Generate secure shares	39
Figure 3.7	Flowchart for Recover shares	40
Figure 3.8	Workflow diagram of the system	41
Figure 3.9	RGBA Image Channels	46
Figure 3.10	AES encryption/decryption algorithm	48
Figure 3.11	MVC Architecture	50
Figure 4.1	Registration Process	54
Figure 4.2	Login Process	55
Figure 4.3	Service Page	56
Figure 4.4	View cart Process	57

List of Figures

Figure No.	Figure Name	Page No.
Figure 4.6	Sending Verification Code process	59
Figure 4.5	Checkout Process	58
Figure 4.7	Verification Process	60
Figure 4.8	generate shares Process	64
Figure 4.9	Open Encrypted CA Image	64
Figure 4.10	View Embed and Encrypted Data	65
Figure 4.11	Open Encrypted Customer Image	65
Figure 4.12	View Embed and Encrypted Data	66
Figure 4.13	Reconstruction Process	66

List of Abbreviations

Abbreviations	Stand For
AES	Advanced Encryption standard
API	Application Programming Interface
BPCS	Bit Plane Complexness Segmentation
CA	Certified Authority
CGC	Canonical gray Code
CVCS	Color Visual Cryptography Scheme
CGI	Common Gateway Protocol
DCT	Discrete Cosine Transformation
DES	Data Encryption Standard
DVCS	Dynamic Visual Cryptography Scheme
EVCS	Extended Visual Cryptography Scheme
HTML	Hyper Text Markup Languages
HTTP	Hyper Text Transfer Protocol
HVC	Halftone Visual Cryptography Scheme
HVS	Human Visual System
J2EE	Java Enterprise Edition
JDBC	Java Database Connecter
JSE	Java Standard Edition

List of Abbreviations

Abbreviations	Stand For
JSP	Java Server Pages
LSB	Least Significant Bit
MVC	Model View Controller
OTP	On Time Password
PBC	Pure Binary Code
PGP	Pretty Good Privacy
PKI	Public key infrastructure
RGB	Red, Green, and Blue
RGBA	Alpha, Red, Green, and Blue
SS	Secret Sharing
SSH	Secure Shell
SSL	Secure Socket Layer
TCP/IP	Transfer Control Protocol/Internet Protocol
TLS	Transport Layer Security
VC	Visual cryptography
VCS	Traditional Visual Cryptography schemes
VSSS	Visual Secret Sharing Scheme
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Table of Content:

الآيــة……I

DEDICATION……..…….....II

AKCNOWLEDGEMENTS…….……..III

ABSTRACT…….IV

الـــــمستخلص…...……..…..….....V

LIST OF TABLES……...…….…....VI

LIST OF FIGURES... ...…….....VII

LIST OF ABBREVIATIONS…….....……X

CHAPTER I: INTORODUCTION.....1

1.1 Introduction:.....2

1.2 The research problem: 3

1.3 The objectives of research: 3

1.4 The methodology of research: 3

1.5 The importance of research: 3

1.6 The boundaries of research:.....4

1.7 The content of research:.....4

CHAPTER II: RELATED WORK AND LITERATURE REVIEW 5

2. Overview: 6

2.1 INTRODUCTION:.....6

2.1.1 Substitution techniques: 7

2.1.2 Transposition techniques: 8

2.2 SYMMETRIC MODEL: 9
2.2.1 Block cipher model: 10
2.2.2 Stream cipher: 13
2.3 ASYMMETRIC CIPHER MODEL: 14
2.4 STEGANOGRAPHY: 15
2.4.1 Modern techniques of steganography: 17
2.4.2 Steganalysis: 20
2.4.3 Steganography attacks: 21
2.5 VISUAL CRYPTOGRAPHY (VC): 21
2.5.1 Traditional Visual Cryptography schemes (VCS): 22
2.5.2 Color Visual Cryptography Scheme (CVCS): 27
2.5.3 Extended Visual Cryptography Scheme (EVCS): 27
2.5.4 Dynamic Visual Cryptography Scheme (DVCS): 28
2.5.5 Applications for Visual Cryptography: 28
2.6 RELATED STUDIES: 30
CHAPTER III: METHODOLOGY, TECHNIQUES AND TOOLS 32
3. Overview: 33
3.1 PART ONE: METHODOLOGY: 33
3.2 PART TWO: TECHNIQUES: 42
3.2.1 Secret Sharing Scheme: 42
3.2.2 Steganography using Alpha channel: 45
3.2.3 Advanced Encryption Standard (AES): 47
3.2.4 Model View Controller (MVC): 49
3.3 PART THREE: SYSTEM TOOLS: 51
3.3.1 Java Enterprise Edition (J2EE): 51
3.3.2 Java Servlet: 51
3.3.3 Java Server Pages (JSPs): 52
3.3.4 NetBeans IDE: 52
CHAPTER IV: RESULTS AND DICUSSION 53
4. Overview: 54

4.1 SYSTEM INTERFACES: 54
4.1.1 Registration Process: 54
4.1.2 Login Process: 55
4.1.3 View and Select Service(s) Processes: 56
4.1.4 View cart Process: 57
4.1.5 Checkout Process: 58
4.1.6 Sending Verification Code process: 59
4.1.7 Verification Process: 60
4.2 SYSTEM ANALYSIS: 61
4.3 RESULTS: 67
4.4 DISCUSSION: 68
4.5 SECURITY ANALYSIS: 68
4.6 COMPARISONS: 69
CHAPTER V: CONCLUSION AND RECOMMENDATIONS 72
5.1 CONCLUSION: 73
5.2 RECOMMENDATIONS: 73
REFERENCES: 75