Impact Factor News

---------- Forwarded message ----------
From: SJIF Impact Factor <evaluation@sjifactor.com>
Date: Sun, 6 Mar 2016 04:45:01 +0000
Subject: Congratulations - SJIF Impact Factor Evaluation [SJIF 2015 = 3.883]
To: Journal of Madenat Alelem College <dr.ayaidkhadem@gmail.com>

Dear Editor/Publisher,

Journal of Madenat Alelem College (ISSN: 2073-2295)

We are pleased to announce that your journal was positively evaluated in the SJIF Journal Rank List evaluation process, which resulted in a score given SJIF 2015 = 3.883 (Scientific Journal Impact Factor Value for 2015).

More and more commonly used rating is the criteria of citation which has also a great impact on gaining the Impact Factor rating. Building citation rating is a long-lasting process which required strict strategy which is consistently inculcated. In that case we would like to invite you to refer back to our Characteristics evaluated criteria.

Our methodology is prepared by SJIF Experts and contains strict recommendations and initiatives which can be taken to improve the Journal. The recommendations will help to gain better scores in different kind of evaluations and especially in gaining better citation results. They will also help the Journal in presenting itself at the international scientific market.

Thank you for requesting SJIF Value for your Journal.

To download your certificate, please login here : http://sjifactor.com/apply.php

Sincerely,

SJIFactor - Scientific Journal Impact Factor
P.O. Box 695, -Chellah
10002,
e-mail : evaluation@sjifactor.com
Website : http://sjifactor.com/

INSTRUCTIONS to AUTHERS

Submitted articles to the Journal of Madinat Al-Elem University College can be published in all fields related to the Academic Departments of the College (Biology, Law, programming Engineering Sciences, Computer Techniques Engineering Law, Medical Physics, Civil Engineering, and Accounting).

Written request for publication and signing a consent form to publish must be for articles which have not been published or submitted for publication to other journals. Three copies with CD are needed. Manuscripts should be typed on: A4 white paper, double spaced, written in Times New Roman font size 14. Margins should be 3cm from top, bottom, left and right. The main title should be in: bold Times New Roman font size 14. Author names should be written in the following sequence: first name, middle name, the family name, followed by the names of departments and institutions of work. A footnote accompanies the first page stating the full address of correspondence author.

Articles need to contain the following items:

- Abstract in English and Arabic not more than 300 words.
- Article includes the following items: Introduction, Materials and Methods, Results and Discussion, Conclusion and References.
- References should be numbered in the text according to the sequence appeared in the text and listed in order.
- Tables and figures should be appropriately titled with size not exceed an A4 page.

The editor reserves the right to reject or accept any article submitted.

Publication charges: Each accepted paper is required to pay the publication charge (100,000 Iraqi dinars). Five thousands Iraqi dinar are requested for each extra page extra printed page.

Contents

	Page
Secret Message Hiding in WAVE PCM Sound File	**5**
Raja Salih , Zaid Sadiq naama , Sherna Aziz Tome	
Smart Antenna Potential on Performance Improvement for Mobile Communication Systems	**17**
Asst. Prof.Dr.Ismail M.Jabber, Asst.Lec.Ansam M. Abed	
Resource Description Framework Schemas for E-Library	**26**
Jamal F. Tawfeq , Saja Majeed Mohammed	
Analysis flow of second order fluid in a vertical channel with porous wall by using the Homotopy Analysis Method (HAM)	**36**
Wala'a Abdul , Mageed Mahdi , Ahmed M. A. Hadi	
Design And Implementation Of A New Hybrid Encryption Algorithm	**49**
Ghada Salim Mohamed	

Secret Message Hiding in WAVE PCM Sound File

Raja Salih
Assist lecturer
Institute of medical technology

Zaid Sadiq naama
Assist lecturer
College of science

Sherna Aziz Tome
Assist lecturer
College of medicine

Abstract

Communications today has been done among millions of users using many application devices like internet or satellite communication channels, the services they can transform many varieties of files like text, images, videos, and audio among different places. Therefore the security of data has been of extreme importance in today's information-based society, including the fields of military, diplomacy, corporation, medicine, and etc….

A form of data hiding is steganography, which is contemporary way for protecting the information by embedding data into digital media for the purpose of copyright, and sending secret messages.

In this paper a scheme of steganography system for hiding secret text message in audio file WAV, (Windows Audio Visual) format is proposed, the hiding mechanism was based on using Low-Bit Encoding (LSB) Least Significant Bit substitution techniques.

To support the immunity of the hiding system, encryption methods with some other support methods (i.e., hiding and hopping) were added to the proposed hiding system, a pseudo random number generator has been designed and implemented to generate non-uniform integer jumps between successive hiding events. The jumps mechanism of the suggested generator is based on the linear feedback shift register of length 23 with feedback function $F(x)=1+X+X^{23}$ produce the maximum period $2^{23}-1= 8388607$.

Keywords: ciphertext**,** cryptography, decryption, encryption , PCM, plaintext, steganography.

إخفاء الرسائل السرية بواسطة الملف الصوتي Wave PCM

رجاء صالح محمد حسن
مدرس مساعد
المعهد الطبي التقني المنصور

زيد صادق نعمه
مدرس مساعد
كلية العلوم للبنات / جامعة بغداد

شيرنه عزيز توما
مدرس مساعد
كلية الطب / جامعة بغداد

الخلاصة

تتم الاتصالات في الوقت الحاضر من قبل ملايين المستخدمين بواسطة أنواع متعددة من التطبيقات مثل الأنترنيت أو قنوات الأتصال عبر الأقمار الصناعية ،وهذه الخدمات من خلالها يمكن تحويل العديد من أنواع الملفات مثل النصوص ، الصور ، وأشرطة الفديو والرسائل الصوتية بين مواقع مختلفة من الكرة الرضية . وبالتالي فأن أمن البيانات وسريتها لها أهمية بالغة وتتطلب عناية قصوى أثناء تداولها في مجتمعات اليوم التي تعتمد على المعلومات والبيانات أساسا لها في المجالات العسكرية ، الدبلوماسية ، الشركات التجارية والمؤسسات الطبية وحتى على مستوى الأفراد.

اقتراح نظام لأخفاء النصوص السرية في صيغة الملفات الصوتية WAV (Windows Audio Visual) وقد اعتمدت آلية الأخفاء بطريقة (LBE) Low-Bit encoding اوتقنيات الإستبدال Least Significant Bit (LSB) .

ولدعم حصانة نظام الإخفاء هذا تم اضافة طرق تشفير أخرى encryptionمع أساليب الدعم الأخرى مثل (الأختباء والتنقل) ، اضيفت هذه الطرق لدعم نظام الإخفاء المقترح وتم تصميم مولد رقم عشوائي زائف لتوليد عدد صحيح غير موحد بين أحداث الأخفاء المتعاقبة .

ان ميكانيكية القفز لمولد عشوائي مقترح يعتمد على مسجل التزحيف ذو التغذية الخلفية الخطية (LFSR) بطول 23 وبدالة تغذية خلفية $F(x)=1+X+X^{23}$ بحيث تولد اعلى قيمة $2^{23}-1=$ 8388607

1- Introduction

Steganograph (literally, covered writing) is the hiding of secret messages within another seemingly innocuous message, or carrier (cover). Digital carriers include email, audio, and video messages, disk space, disk partitions, and images [1].

The subjective quality of the audio data depending on our hearing sense could not recognize all voices and noises that are accompanied with original wave media. Data hiding in audio signals are especial challenge, because the (HAS) Human Auditory System operates over a wide dynamic range. The HAS perceives over a range of power greater than billion to one and range of frequencies greater than one thousand to one.[2]

Sensitivity to additive random noise is also acute. When performing data hiding on audio, one must exploit the weakness of the HAS, while at the same time being aware of extreme sensitivity of the human auditory system. [3]

In this research has been the builder a hiding system of secret messages in wave files without producing any significant distortion

2 –Least Significant Bit Encoding (LSB)

Low-bit encoding is the simplest way to embed data into other data structure. By replacing the least significant bit of each sampling point by a code binary string, we can encode a large amount of data in an audio signal. The bit rate will be 8 Kbps in an 8KHz sampled sequence and 44Kbps in a 44KHz sampled sequence.[4]

The simple algorithm of LSB for low-bit encoding is as follows :

- Represent the object as vector of integers.
- Change the least significant bit in either all or some integers to represent a 1 or 0 in the mark

Depending on the amount of embedded information and the amount when the wave media carries, it is quite unperceivable. For example the first thing to do is to hide an ASCII code of A, which represent 01000001, and then part of wave media cover data will be

(11101011 10001011 10101010 11001010 10001010 10111101 11111111 01001111)

After information is hidden the wave file will be

(1110101**0** 10001011 10101010 11001010 10001010 10111100 11111110 01001111)

3 - Wave PCM Sound file Format

The most popular waveform coding technique used to present the human speech using Pulse Code Modulation (PCM).[3]

The WAVE file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. A (RIFF) resource enter change file starts out with a file header followed by a sequence of data chunks as shown in figure (1). A WAVE file is often just a RIFF file with a single "WAVE" chunk which consists of two sub-chunks—a "fmt" chunk specifying the data format and a "data" chunk containing the actual sample data which is the "canonical form". As shown on table. (1)

File offset (byte)	Field name	Field size (byte)	The RIFF chunk descriptor
0	Chunk ID	4	The "RIFF" chunk descriptor The format of concern here is "WAVE ", which requires two sub-chunks:"fmt" and "data"
4	Chunk size	4	
8	Format	4	
12	SubChunk1ID	4	The "fmt" sub-chunk Describes the format of the sound information in the data sub-chunk
16	SubChunk1size	4	
20	Audio Format	4	
22	Num Channels	2	
24	Sample Rate	2	
28	Byte Rate	4	
32	Block Align	2	
34	Bit spersample	2	
36	SubChunk2ID	4	The "data' sub-chunk Indicates the size of the sound information and contains the raw sound data
40	SubChunk2size	4	
44	Data	Subchunk2size	

Figure (1) The Canonical WAVE file format [4]

4 - Linear Feedback Shift Register

A commonly used method for generating binary sequences, especially pseudo-random sequences, is to feed a binary function of the state of a shift register back to its input. The stages of shift register serve as the input of logical circuit whose output is connected to the input of the shift register. Shown in figure (2)

An n-stage shift register $s_0, s_1, \ldots, s_{n-1}$. The contents of the stages change in time with a clock pulse according to the rule:

Let $S_i(t)$ denote the content of si after the t^{th} time pulse ($t=0,1,2,\ldots$).

$S_{n-1}(t+1)=f(c_0 s_0(t), c_1 s_1(t), \ldots c_{n-1} s_{n-1}(t))$, where the c_i are all specified as 0 or 1.

The function build is called the feedback function of the register and if $f(s_0,s_1, \ldots,s_{n-1})=c_0s_0+c_1s_1+\ldots+c_{n-1}s_{n-1}$ then the register called linear register. This is represented by the $c_i=1$ denotes a closed connection and $c_i=0$ an open one.[6]

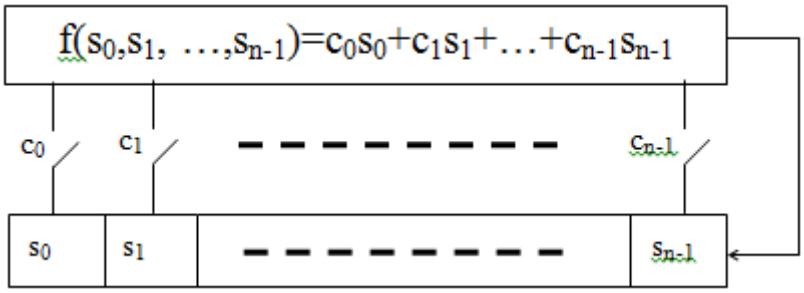


Figure (2) : Linear feed back shift register

A assume $c_0=1$ so that $s_{n-1}(t+1)$ is dependent on $s_0(t)$. Let $s_t=s_0(t)$, an infinite binary sequence denoted s_t satisfy the linear recurrence relation as $s_{t+n}=\sum_{i=0}^{n-1} c_i s_{t-i}$, for t=0,1,….n.

The shift register has been identified as characteristic polynomial as shown [8].

$F(x)=1+c_1x+c_2x^2+\ldots+c_{n-1}x^{n-1}+x^n$ (remembering $c_0=1$).

5 - Cryptography

Steganography is a way that deals with finding the best place in cover media to hide data.If the data encrypted before hiding it, this will give more security immunity to the cover data.

In this paper research, before hiding the secret data were encrypted by using stream cipher generator. [7]

5.1 - Stream Cipher

One of the cryptographic primitives used to ensure secure communication over public and unsecured channels (such internet, mobile) is the stream cipher. In a stream cipher the plaintext is encrypted on bit by bit basis. In the encrypting of data flow transmitted, the key is fed into an algorithm called running key generator (RKG) to generate a long pseudorandom binary sequence. This “Key Stream” is then mixed with the plaintext sequence, usually by using exclusive-or (XOR bitwise module 2 additions) logic gate, to produce the cipher text. A typical stream cipher is shown in figure (3)

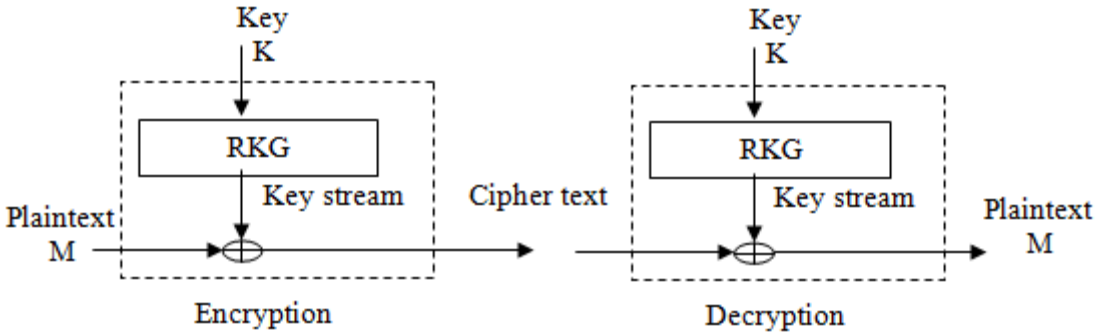


Figure (3) Stream Cipher

A common type of RKG employed in stream cipher system consists of n (mostly maximum length) LFSRs whose output sequences are combined in a nonlinear function F to produce the key stream.[7]

5.2- Encryption and Decryption

Cryptographic algorithm have been carefully designed for maximum security, it divide into two subsystem:

Driving subsystem, which are consists of 8-LFSRs with maximum period are corresponding feedback polynomials

$F_1(X)=1+X^{13}+X^{33}$ $F_2(X)= 1+X^3+X^{31}$

$F_3(X)= 1+X^2+X^{29}$ $F_4(X)= 1+X^3+X^{28}$

$F_5(x)= 1+X^3+X^{25}$ $F_6(X)= 1+X^5+X^{23}$

$F_7(x)= 1+X^{14}+X^{17}$ $F_8(X)= 1+X^{14}+X^{17}+X^{18}+X^{19}$

The second subsystem is non-linear compost combining subsystem F. which represent a 2D matrix 16x8 bits each bit addressed by driving subsystem, the output determined through the intersection of row by first 4 LFSRs (0..15 row) and column by next 3 LFSRs (0..7 row) the result mixed with the output of the register 8 using x or to produce the key sequence, as shown in figure (4)

6 -

original code 6bit			b_5	b_4	b_3	b_2	b_1	b_0
	b_5	b_4	b_3	b_2	b_1	A_0		
	b_5	b_4	b_3+b_5	b_2+b_4	b_1+b_3	$b_0 + b_2$	b_1	b_0
New extended code 8bit	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0

Cryptographic Algorithm

Build a coding table of 6-bit has been build of printable keyboard characters as in the coding table(1). The basic key is 16-character of 6-bit extended into 8-bit by using the original character shift left 2 bits and x.

Example:

After extended the basic key ino 128 bits we use this bits to initial the driving and the nonlinear combining parts, each shift of driving subsystem will produce one bit output from combining and then to produce key bit.

original code 6bit			b_5	b_4	b_3	b_2	b_1	b_0
	b_5	b_4	b_3	b_2	b_1	A_0		
	b_5	b_4	$b_{3+}b_5$	b_2+b_4	b_1+b_3	$b_0 + b_2$	b_1	b_0
New extended code 8bit	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0

dec	code	binary	dec	code	Binary	Dec	code	binary	dec	code	binary
0	S	000000	16	T	010000	32	f	100000	48	3	110000
1	q	000001	17	9	010001	33	C	100001	49	d	110001
2	t	000010	18	/	010010	34	8	100010	50	J	110010
3	p	000011	19	m	010011	35	7	100011	51	H	110011
4	x	000100	20	Q	010100	36	O	100100	52	k	110100
5	g	000101	21	c	010101	37	n	100101	53	L	110101
6	0	000110	22	y	010110	38	G	100110	54	K	110110
7	w	000111	23	u	010111	39	X	100111	55	E	110111
8	R	001000	24	i	011000	40	Z	101000	56	6	111000
9	o	001001	25	b	011001	41	5	101001	57	V	111001
10	B	001010	26	M	011010	42	D	101010	58	e	111010
11	l	001011	27	v	011011	43	P	101011	59	r	111011
12	z	001100	28	W	011100	44	I	101100	60	space	111100
13	A	001101	29	F	011101	45	a	101101	61	h	111101
14	4	001110	30	1	011110	46	s	101110	62	j	111110
15	Y	001111	31	N	011111	47	2	101111	63	U	111111

Table (1) Cryptographic Algorithm

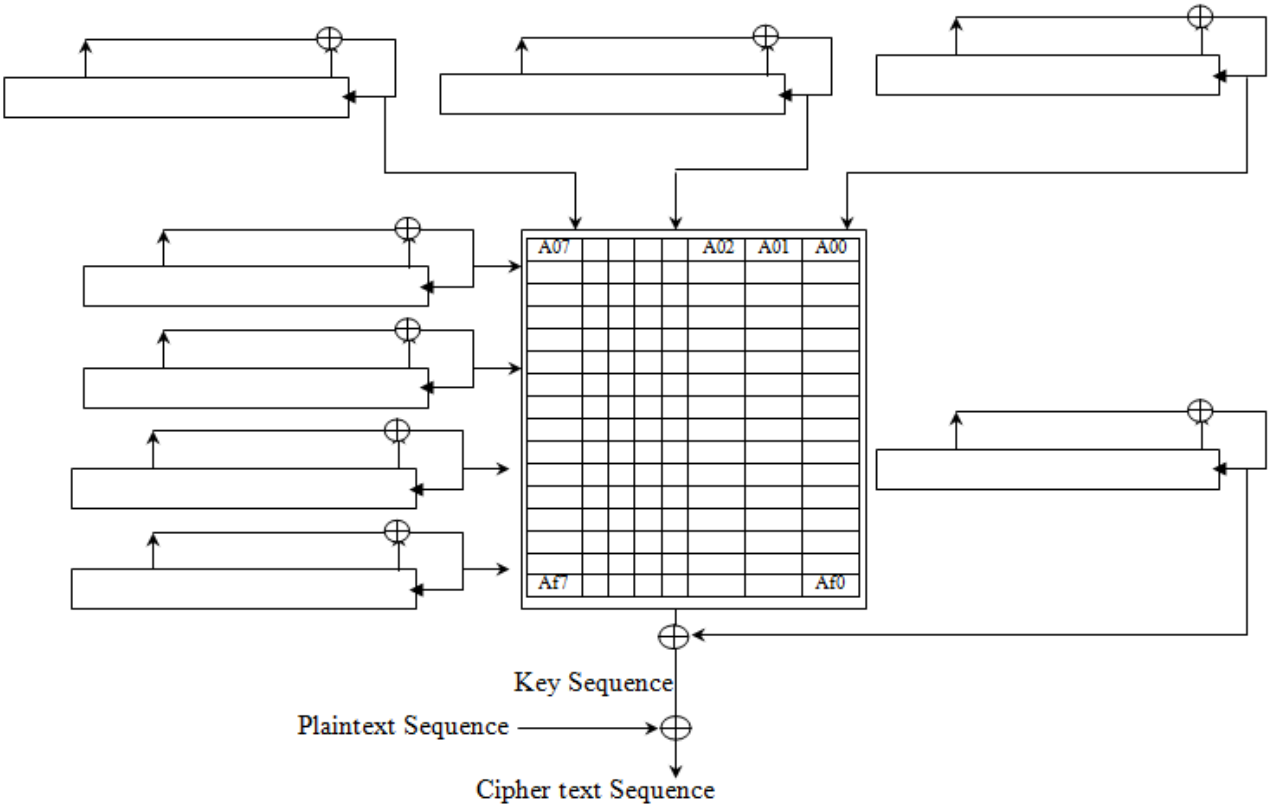


Figure (4) Cryptographic mechanism

7 - Hopping and Hiding

If the data embedding is done sequentially over the entire wave file (i.e. hiding in byte after byte), will make the stego system very vulnerable against simple tools of steganalysis. Therefore jump with variable (pseudo-random) length between successive hiding events will greatly increase the security level of stego system. In this research a pseudo random number generator was designed and implemented to generate non-uniform integer jumps between successive hiding events. The jumps mechanism of the suggested generator is based on the linear feedback shift register of length 23 with feedback function $F(x)=1+X+X^{23}$ produce the maximum period $2^{23}-1=8388607$.[9]

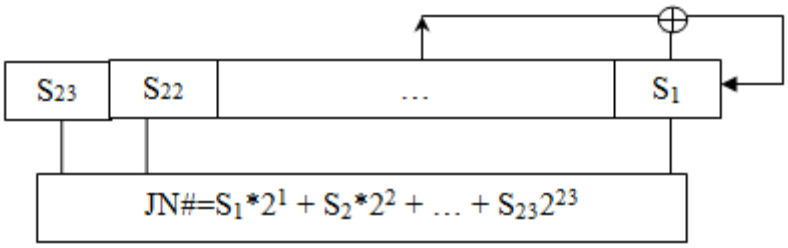


Figure (5) : The jumps mechanism

The Algorithms of the proposed system :-

Hiding poses

Step 1 : read plan text

Step 2: split play text into an ASCII

Step 3 : covered each ASCI info eight bits

Step 4 : read he decimal six, bits key

Step 5 : shift key char 2 bit

Step 6 : hopping the eight bits with R key G inside audio cover

Step 7 : hide the cipher text bit in the LSB of determined Audio byte

Step 8: if plan file finished

go to step 9 etc

go to step 6

extracting process

step 9 : hopping inside Audio file (cover)

step 10 : mask with LSB of determined audio byte and extract the cipher text bit

step 11 : extract hix decimal key of six bits code

step 12 : shift key char 2 bit left then mixed it with the original by using XOR

step 13: collect bit into ASCII code

step 14 : if cipher text finished

go to step 15 etc

go to step 9

step 15 : end

8 - The proposed system

The block diagram explains how to hide the message and how to extract it shown in figure (6)

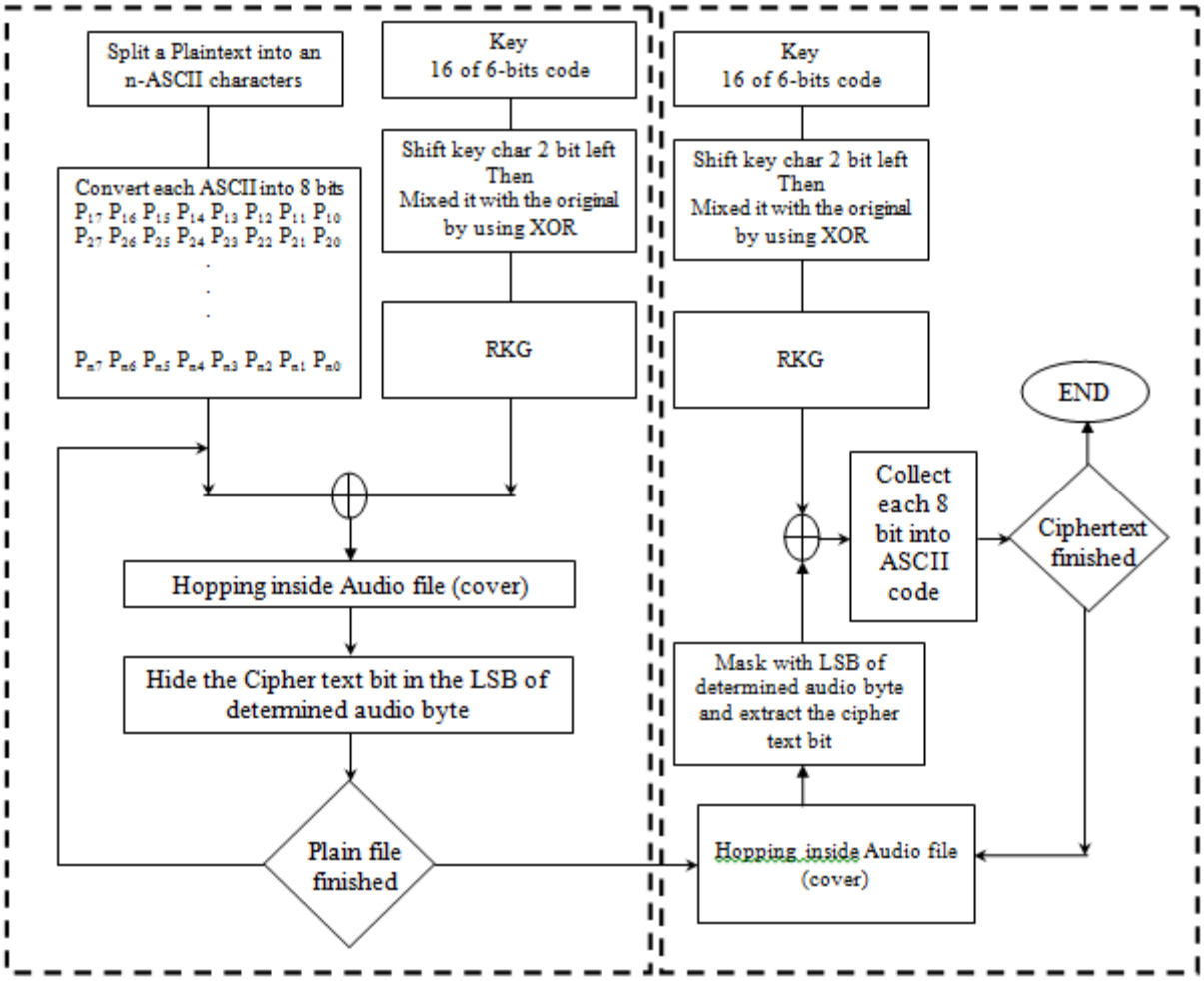


Figure (6) The block diagram of proposed system

9 - Fidelity Criteria

Signal-to-noise (SNR) measures are estimates of the quality of a quality reconstructed image compared with an original image. Reconstructed images with higher metrices are judged better quality. Traditional SNR measures do not equate.

First compute the mean squared error (MSE) of the reconstructed audio as follows:

$$MSE = \text{MSE} = \frac{\Sigma[f(I,j)-f^*(I,j)]^2}{N^2} \quad \ldots\ldots\ldots\ldots(1)$$

The summuation is over all signals. The root mean square error (RMSE) is the square root of MSE.

PSNR in decibels (dB) is computed by using:

$$PSNR = 20\text{PSNR} = 20\log10 \frac{(L\text{-}1)^2}{\text{RMSE}} \quad \ldots\ldots\ldots\ldots(2)$$

L: Max Value

$$20\text{SNR} = 20\log10\left(\frac{\text{Max value}}{\text{RMSE}}\right) \quad \ldots\ldots\ldots(3)$$

Mean absolute error (MAE) can the measure the quality to the different of a reconstructed audio compared with one original audio, the value of this measure be between 1 and 0, the actual value be good if the value near from zero.

$$MAE = \text{Bit Per Sample} \quad \text{BPS} = \frac{\text{Hidden data Bit}}{\text{Total Cover size (sample)}} \ldots\ldots\ldots\ldots(4)$$

Typical PSNR values range will be greater than or equal to 50 .They are usually reported to two decimal points (e.g 25.47). The actual value is not meaningful, but the comparison between two values for different constructed audio signals gives one measure of quality. An informal threshold of 0.5 dB PSNR is used to decide whether to incorporate a coding optimization because they believed that an improvement of that magnitude would be visible.

The data hiding in wave data, and samples, the following table (2) illustrates the PSNR, MSE, and BPS results for eight types of data with different sizes are hidden in a “boop.wav” file whose size is (79561).

“boop” file whose size is (64162 byte).					
File	**Length(byte)**	**MSE**	**PSNR**	**BPS**	**SNR**
1	**1925**	**0.01**	**68**	**0.19**	**66**
2	**3208**	**0.02**	**65**	**0.32**	**64**
3	**6416**	**0.04**	**62**	**0.64**	**61**
4	**8341**	**0.05**	**61**	**0.83**	**59**
5	**10266**	**0.07**	**60**	**1.03**	**58**
6	**12832**	**0.08**	**59**	**1.29**	**57**
7	**17324**	**0.1**	**58**	**1.74**	**55**
8	**19249**	**0.11**	**58**	**1.93**	**55**

Table (2) : Output result of MSE,BPS, SNR and PSNR

The general structure of the proposed system is illustrated in figure (6) it consists of two basic modules: hiding and extraction modules . The input to this system are the cover file (wave file) and secret file (binary file) . These input are processed in the hiding part with various operations to produced stego wave file . The stego audio entered to extraction stage is processed through a set of operations to retrieve the secret data.

10- Conclusions:-

From the test results listed in propose system the following remarks wave derived

1- Hiding in voiced block sample is more suitable to avoid noise occurrence which is more probably happen when unvoiced blocks are used as host area.

2- Large threshold value provide more power in cover audio signal by avoiding unvoiced blocks and increased correct retrieved bits but decreased in hiding.

3- The results show acceptable hiding performance and the quality of reconstructed wave file is not subjectively different from the original wave.

11-References:

1- **Roue**, B. and Chassery, J. (2004) Improving LSB steg analysis using marginal and joint probabilistic distribution, *Proceeding of the 2004 workshop on Multimedia and security*. ACM New York, NY, USA, pp.75-80, 2004.

2- **Dumitrescu**, S., Wu, X., Wang, Z. (2003) Detection of LSB steganography via sample pair analysis, *IEEE Transactions on Signal Processing*, Vol.51, No.7, pp.1995-2007, 2003.

3- **Gary** C. Kessler (2004) An Overview of Steganography for the Computer Forensics Examiner, *Forensic Science Communications*, Vol.6, No.3.

4- **Wang**, H. Wang**, S. (2004)** Cyber warfare: steganography vs. steganalysis. *Communications of the ACH* Vol 47 No. 10.

5- **Menezes**, A.J Oorschot, P.C., Vanstone,S.A. (2007) *Handbook of Applied Cryptography*, CPC Press, NY.

6- **Katzenbeisser**, S., Fabian A.P. (2000) Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House Publishers. London.

7- **Lu** P., Luo, X.,Tang Q., Shen Li. (2004) An improved sample pairs method for detection of LSB embedding", *Proceedings of the 6th Information on Information Hiding Workshop*, Berlin ,pp 116-127.

8- **Johnson**, N. F., Duric, Z. and Jajodia, S. (2001) *Information Hiding: Steganography and Watermarking: Attacks and Countermeasures*. Kluwer Academic, Norwell, Massachusetts.

9- **Wayner**, P. (2009) *Disappearing Cryptography: Information Hiding: Steganography & Watermarking*. 3rd ed., Morgan Kaufmann, San Francisco, California.

Smart Antenna Potential on Performance Improvement for Mobile Communication Systems

Asst. Prof.Dr.Ismail M.Jabber

University of Madenat AL-Elam

Amin_ck87@yahoo.com

Asst.Lec.Ansam M. Abed

University of Madenat AL-Elam

ama_ansam@yahoo.com

Abstract

Smart antennas have numerous important benefits in mobile communication systems. Smart antennas can provide higher system capacities by directing narrow beams toward the users of interest, while nulling other users not of interest. This allows for higher signal-to-interference ratios, lower power levels, and permits greater frequency reuse within the same cell. This, in turn, increases the system capacity and the quality of services.

In this paper we analyze the effect of base-station sensitivity obtained by using smart antenna to increase capacity and reduced the mobile transmit power at different loads scenarios.

Key words: Smart antennas, communication systems, mobile.

ملخص البحث

للهوائيات الذكية إمكانيات مهمة في تحسين أداء شبكات الهاتف النقال. بإمكان الهوائيات الذكية أن تعطي منظومات اتصال بسعة عالية وذلك بتوجيه حزم ضيقة باتجاه المشترك المطلوب الاتصال به وتصفير اتجاه مصادر التداخل.

وهذا يؤدي لزيادة نسبة قدرة الإشارة إلى التداخل مما يسمح بإعادة استخدام الترددات بشكل اكبر وهذا بدوره يزيد من سعة المنظومة ونوعية الخدمات .

في هذا البحث قمنا بتحليل تأثير حساسية محطة القاعدة التي يمكن الحصول عليها باستخدام الهوائي الذكي لزيادة السعة وتقليل القدرة المرسلة بوحدة المشترك باستخدام سيناريوهات أحمال مختلفة للنظام .

1. Introduction

As the number of cellular subscribers continues to grow rapidly, service providers are forced to increase the capacity of their networks especially in populated areas. Increasing capacity is of prime importance to serve a large number of subscribers at the same time [1].

Mobile communication system capacity can be increased in several ways. These include enlarging the total bandwidth allocated to the system, reducing the channel bandwidth through efficient modulation, decreasing the number of cells in a cluster, and reducing the cell size through cell splitting or sectorization [2,3].

It is expensive for the service providers to get additional spectrum with high license fees that must be paid. Reducing the cell size means many new base stations have to be built, with additional costs and results in more numbers of handoff. Cell sectorization provides greater possibility of reusing a frequency channel by reducing interference across the original cell, but it results in more frequent handoffs, which requires greater system resources to support and coordinate [4].

One of the important strategies for increasing capacity are interference reduction on the downlink and interference rejection on the uplink. Interference can be rejected by focusing the transmitted energy along the direction of the intended users using directional beams or by forming nulls in the direction of interfering sources.

The use of high gain narrow beams antennas improve carrier to interference ratio (C/I) , thus reduces frequency reuse factor for the same quality of service. Lower frequency reuse factor means more channels per cell, i.e., higher capacity. This can be accomplished by using smart antennas at the base to direct the electromagnetic energy to the intended users [5].

This paper concentrates on techniques for increasing capacity using smart antennas.

2. Smart Antenna Theory

The smart antenna combines multiple antenna elements (antenna array) with an adaptive signal processing capability to optimize its radiation and/or reception pattern in response to the signal environment.

The idea of smart antennas is to direct a single beam to each user to optimize the radio performance as shown in Figure(1). Using smart antenna with M elements will increases the signal amplitude (M) times because the desired signal received at each antenna element is phase-shifted due to weight coefficient, and then the signal components from each element are positively combined [7] [6].

The gain provided by smart antennas can extend the range of a cell to cover a larger area and more users than would be possible with omnidirectional or sector antennas [1].

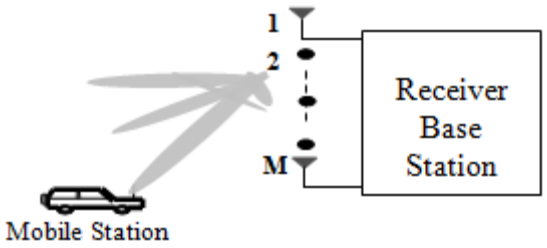


Figure 1. Smart Antenna Theory

Interference reduction can be implemented using high gain narrow beams to communicate with mobiles on the downlink, a base station is less likely to interfere with nearby co-channel base stations than if it used an omnidirectional antenna. Theoretically, the number of cells per cluster can be decreased, increasing spectral efficiency and capacity [2].

3. Smart Antenna Potential in Improving Capacity

Smart antennas can be used to allow the subscriber and base station to operate at the same range as a conventional system, but a lower power. This permit channels frequency reuse more frequently than conventional systems using fixed antennas, since the carrier-to-interference ratio (C/I) is much greater when smart antennas are

used. Ability to tighten frequency reuse allocates many channels per base station, and long range associated by smart antennas due to high gain [7].

The minimum RF level at the receiver input is referred to as the receiver threshold sensitivity level. At this level, the signal is only just above noise-level and is not very intelligible. If the radio-base station sensitivity can be reduced, this would be translated into a capacity increase and reduced mobile transmitted power.

If P_c is the carrier power, N is the noise, and I be interference power, then the receivers sensitivity (S) , can be given by [7] :

$$S = \frac{P_c}{N+I} \qquad (1)$$

The cell load (α) can be shown to be

$$\alpha = \frac{I}{N+I} \qquad (2)$$

where I denotes the other-cell interference and the same-cell interference.

Reducing the load factor for a given number of users or sector throughput improves both coverage and capacity.

If the smart antenna lower the receiver's sensitivity requirement to S', a capacity increases of (β) and a power reduction of (δ) can be achieved, as follows [7]:

$$S' = \frac{P_c}{N'+I'} = \frac{\delta P_c}{(1-\alpha)(N+I)+\beta\delta\alpha(N+I)} \qquad (3)$$

It follows that the capacity gain and the power reduction are given by :

$$\beta = \frac{\delta(S/S')+\alpha-1}{\delta\alpha} \qquad (4)$$

$$\delta = \frac{1-\alpha}{(S/S')-\beta\alpha} \qquad (5)$$

If the capacity is increased ,the system load will also increase. When the transmitted power is reduced , the battery life of the mobile is extended. On other hand ,with the same mobile transmitted power, this could be translated into a range extension [6,7].

4. Smart Antenna Simulation Results and Discussion

4.1 Power Reduction Using Smart Antenna

In Figure (2), the power reduction (δ) is plotted as a function of the gain that can be achieved using smart antenna (10 Log M), for different load factors (25%, 60 %).

In 60% loaded system, a 5.0 dB in the receiver's sensitivity could lead to a 8.0 dB power reduction. The same receiver sensitivity could lead to a 5.9 dB in 25% loaded system.

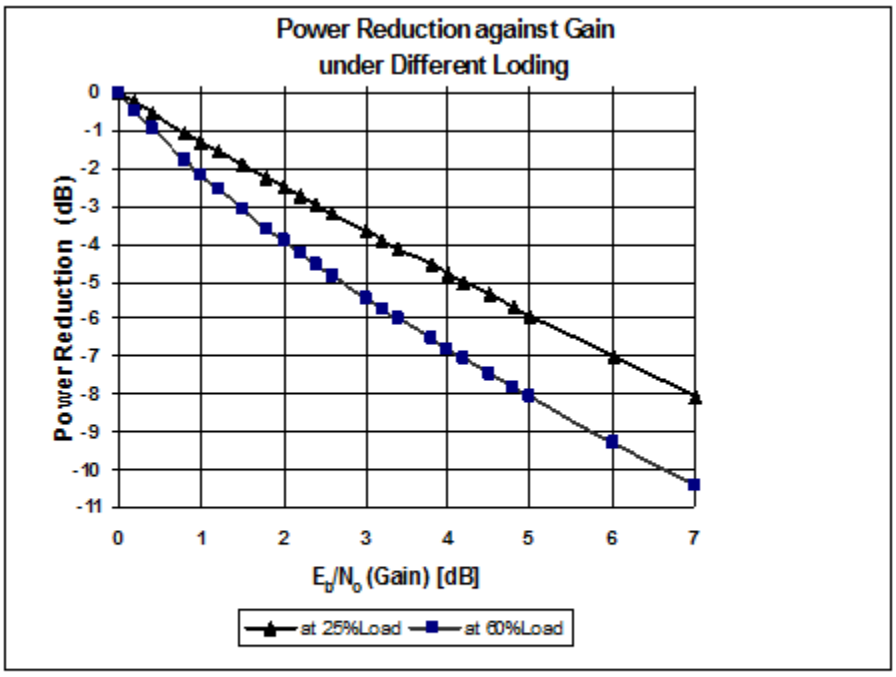


Figure (2) Power Reduction and Gain with Smart Antenna under Different Loading Scenarios

If smart antennas are used to allow subscribers to transmit less power for each link, then the Multiple Access Interference (MAI) is reduced, which increases the number of simultaneous subscribers that can be supported in each cell.

If the received power requirement at the mobile remains the same, with M-element array at the base station, the output power from amplifiers are reduced .Optimizing transmission toward the wanted user achieves lower power consumption and amplifier costs, since the hardware components of the high-power amplifiers are expensive.

Figure (3) shows that as the distance increases, the received signal becomes weaker. When a subscriber unit transmits 0.6 watt (27.78 dBm), the power received at a base station located 2 km a way from the mobile unit will receive (-78.638 dBm), when using omnidirectional antenna , while it will be (-69.608 dBm), when array of eight elements is used at the base station. The difference is due to the gain obtained by using the array (10 Log 8 = 9.03 dB).

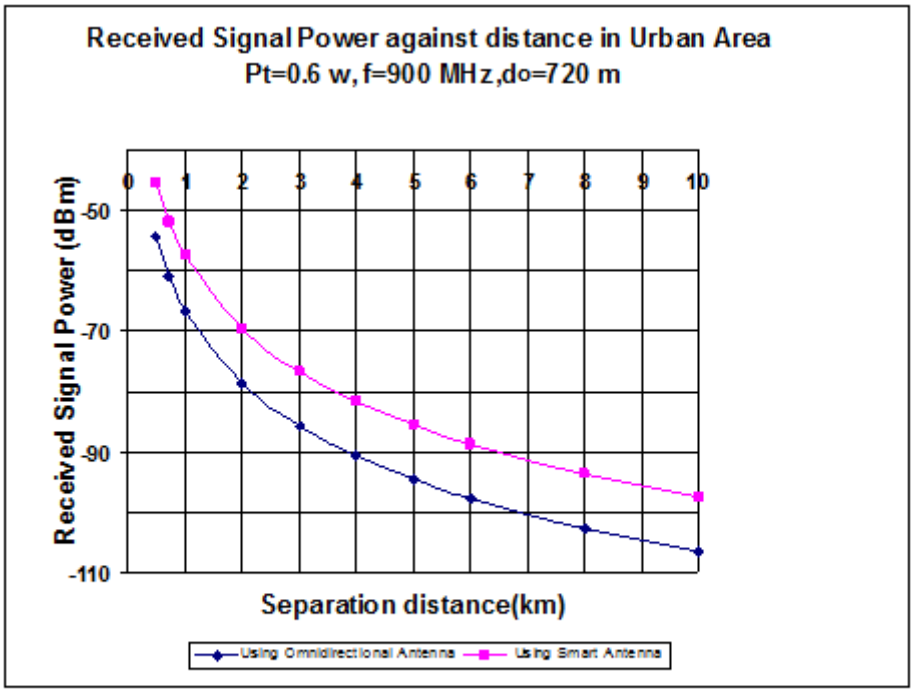


Figure (3) The Received Signal Power against Distance Using Omnidirectional and Smart Antenna

4.2 Increasing of Capacity

Figure (4) shows the expected capacity increase that can be achieved with no power reduction.

It can be noticed that a 3 dB gain with 60% loaded system corresponds to 166% capacity increase.

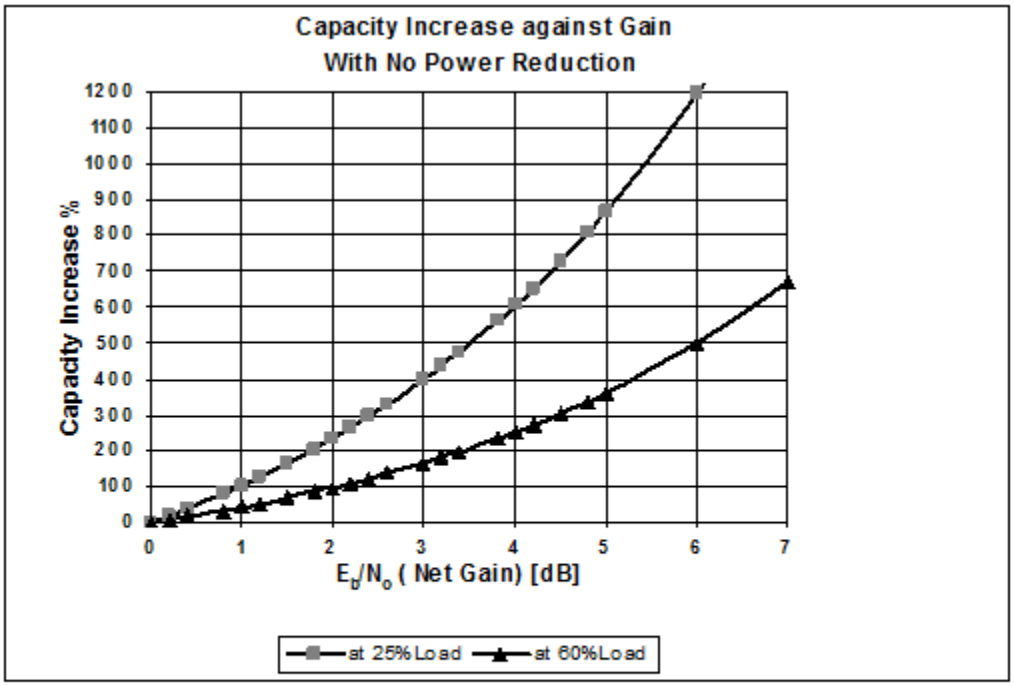


Figure (4) Capacity Increase as a Function of the Gain with Smart Antenna under Different Loading Scenarios without Power Reduction

In Figure (5), we have plotted capacity increase in 50% loaded system, for 50%, and 0% power-reduction factors. It can be seen that for a 3 dB gain, power can be reduced by 50% and capacity will increase by 33 %. A capacity improvement of 110 % could be obtained with a 4 dB gain at the same scenario. From the figure it can be seen how capacity and power reduction can be traded off.

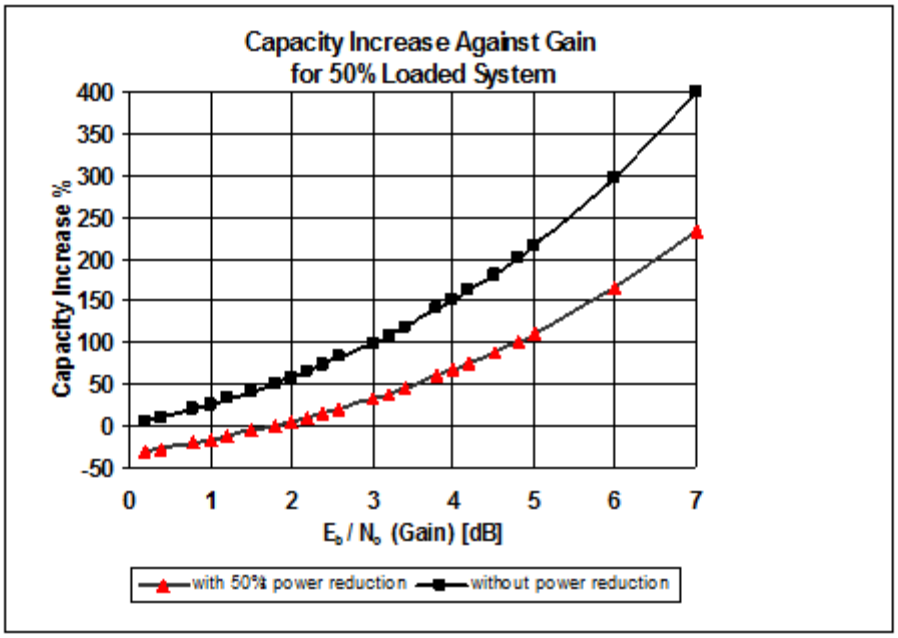


Figure (5) Capacity Increase as a function of the Gain with Smart Antenna of 50% Loading System, with 50%Power Reduction

5. Conclusion

The potential of smart antenna in improving mobile communication performance in terms of range and capacity is studied. The results obtained has been shown that reduction base station sensitivity requirement would be translated to a capacity increase and/or reduced mobile transmit power.

Concluded that with smart antennas at the base station, we can increase the uplink capacity by raising the uplink target load factor without sacrificing coverage because the reduction in array gain can limit the interference level and improve coverage.

References

1- **Sallomi**, Adheed Hasan. (2007) Smart Antenna Performance Analysis for Mobile Communications in Urban Environments. a thesis presented to the university of technology, Baghdad.

2- **Rappaport** ,S. (1997) Theodore and Blankship, Keith. Propagation and Radio System Design Issues in Mobile Radio Systems, Virginia polytechnic Institute.

3- **Sallomi**, Adheed H, and Salim, Sana R. (2009) Range –Coverage Extension Using Smart Antennas in Mobile Communication Systems. Iraqi Journal of Applied Physics, Vol. 5, No.2, PP25-28.

4- **Krzysztof**, Wesolowski. (2002) Mobile Communication Systems, Jhone Willy and Sons Ltd, First Edition.

5- **Bailey**, David. (2003) Practical Radio Engineering and Telemetry for Industry Gross", First Edition, Linacre House, Oxford.

6- **Balanis** C.A. (1997) Antenna Theory: Analysis and Design, 2nd Edition, John Wiley and Sons, New York.

7- Zooghby, A. H. (2001) Potentials of Smart Antennas in CDMA Systems and Uplink Improvements," IEEE Antennas and Propagation Magazine, Vol. 43, No. 5, pp. 172–177.

Resource Description Framework Schemas for E-Library

Jamal F. Tawfeq
PhD Computer Science
University College Madenat Al-Elem
drjamal2004@yahoo.com

Saja Majeed Mohammed
MSc. Computer Science
Baghdad University
saja.mohammed82@yahoo.com

Abstract

Libraries can play a major role in the dissemination of knowledge as a huge repository of knowledge. This research shows the description for the content of the electronic library using metadata and Resource Description Framework (RDF) to facilitate access to content at any time based on this description, thus providing a more meaningful search. In this paper provides an integration of computer science techniques with electronic libraries, and determination of semantic features of this content by proposing a new scheme representative in the Resource Description Framework (RDF) and modification of the basic elements in RDF Dublin core.

Keywords: Digital-library, Semantic Web, Metadata, RDF, RDFS.

وصف محتوى المكتبات الالكترونية باستخدام البيانات الوسطية

سجى مجيد محمد[1]، جمال فاضل توفيق[2]

1. **قسم علوم الحاسبات، جامعة بغداد**
2. **قسم علوم الحاسبات، كلية مدينة العلم الجامعة.**

الخلاصة

يمكن للمكتبات أن تلعب دورا كبيرا في نشر المعرفة كونها مستودعا ضخما من المعرفة. يوضح هذه البحث وصفا لمحتوى المكتبة الإلكترونية باستخدام البيانات الوسطية وإطار وصف الموارد لتسهيل الوصول للمحتوى في أي وقت باستخدام هذا التعريف، وبالتالي توفير بحث أكثر جدوى. ويناقش هذا البحث كيف يمكن دمج تقنيات علوم الحاسبات مع المكتبات الإلكترونية، وكيف يمكن تحديد السمات الدلالية لهذا المحتوى من خلال اقتراح مخطط جديد ممثل في إطار وصف الموارد و تعديل العناصر الأساسية في دبلن آ ر دي أف.

1. Introduction

The World Wide Web is the biggest sources of information, including documentation and information sources and variety that can be accessed through traditional search engines. There is a number of difficulties for finding exact ones supposed to be shown to somebody. The metadata is the solution of the problem of resource discovery on the Web.

Libraries are the main source of information for the users, therefore the digital library can be defined as " a focused collection of digital objects that can include text, visual material, audio material, video material, stored as electronic media formats (as opposed to print, microform, or other media), along with means for organizing, storing, and retrieving the files and media contained in the library collection".[1]
The benefits of digital libraries are the following:

- Easy to bring the information to the end user, unlike the traditional library.
- Provides infinite storage with low cost.
- No need to physical space or boundary.
- Available at any time.
- Provide multiple and universal accesses.
- Simplest to maintenance.

1.2 What is The Semantic web?

In Web the information should be more machine understandable, So The Semantic Web can bring structure to the meaningful content of Web pages, creating an environment where software agents roaming from page to page can readily carry out sophisticated tasks for users". [2]
Also, the semantic web technology provides a data which can be reused in many applications; it is implemented by the Resource Description Framework (RDF).

1.3 Semantic Digital Libraries

The use of semantic technology in a digital library can improve the precision of search engine, enhance the architecture, expanding in the data repository and archives, the discovery of information to make the users can easily find the information . The "Semantic search encapsulates a concept-based, semantic matching and ontology-centric framework for providing extant search results".[3]

Also, " The benefit of the semantic approach based on ontologies is that it gives us a framework for searching and browsing information objects on the web and gives more relevance and accuracy to search processes. ".[4]

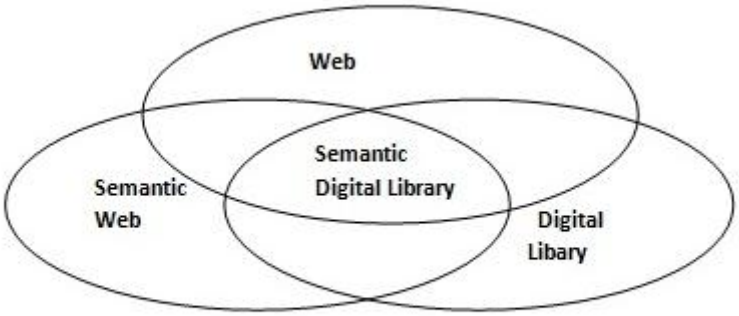


Figure 1.The process of representing a semantic digital library

2. Metadata Concept

Metadata is Structured Document about document, objects, photos, and books, when properly implemented metadata can unambiguously describe information resource, enhancing information retrieval and enabling accurate matches to be done.

Metadata are used to describe data, information and any resource. it can describe just about any thing you find on a computer. Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage information resource[2]. In this paper the information resource is Books.

T. B. Lee give a well-formed definition to metadata as [3][4]:

2.1. Definition

Metadata is machine understandable information about web resource or other things.

Books metadata is structured information about book. Such as titel, auther , edition, publishing, and so on.

Throughout the search in this paper, it was founding that, there are three principles for book metadata:

1. Metadata is essential to identify and track the book.
2. Ownership metadata must never be removed.
3. Metadata must be written in formats that are understood by all.

If all application writes metadata using open standards that are fully consistent and interoperable, then information will be able to move seamlessly between different system and environments."Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information". [5]

2.2. Dublin Core Metadata Element Set

" The Dublin Core is meant to be sufficiently simple to be understood and used by the wide range of authors and casual publishers who contribute information to the internet. Dublin Core elements have become widely used in documenting Internet resources". [6]

- Title
- Author or Creator
- Subject and Keywords
- Description
- Publisher

- Other Contributor
- Date
- Resource Type
- Format
- Resource Identifier
- Source
- Language
- Relation
- Coverage
- RightsManagement

3. RDF and RDF Schemas

RDF (Resource Description Framework) is the primary technology for the semantic web implementation which is "developed by W3C are standard web ontology languages for implementing the Semantic Web". [7]

The RDF is represent and exchange the information on the web, RDF is composed from triple structure (resource , properity , value) which represent a statements about resource.

Assume this example of statements:

"http://www.example.org/index.html has a creator whose value is John Smith

could be represented by an RDF statement having:

- resource is a (subject) http://www.example.org/index.html.
- properity is a (predicate) creator.
- and a value is an (object) is John Smith.

RDF statementscan be represented as nodes and arcs in a graph:

- A nodes for the subject and the object.

An arc for the predicate, directed from the subject node to the object node".[6]

Figure 2. represent the RDF statement above in a graph

The RDF/XML to this graph is:

```
<rdf:RDF>
    <rdf:Description    rdf:about= http://www.example.org/index.html >
        <creator>John Smith</creator>
    </rdf:Description>
</rdf:RDF>
```

The RDF has vagueness . To clear this limitation, the RDF Schema is required.The RDF schema is a Worldwide language developed by W3C (World Wide Web Consortium) for making ontology in RDF and for describing the the metadata structure to illustrate the WWW resources by using personal vocabularies .

4. RDF Library Schemas

These schemas are:

a. Modify Dublin Core Matadata elements

The Dublin Core Metadata element set for the digital library bibliographic search information is modified as below:

- **Title**: Title of the book.
- **Description**: Summary of the content of the book.
- **Author**: An entity associated with the creation of the book.
- **Publisher**: An entity responsible for making the book available.
- **Date:** A point or period of time associated with the publishe of the book.
- **Language**: The native language of the book.
- **Rights:** Copyright of the book.
- **Format:** The data format(e.g., pdf , word) of the resource.
- **Subject:** The topic of the content of the book. It could be one keyword or more to describe the book.
- **Type:** Field of this resource.
- **Keywords:** a keyword means any word that you wish to find in the book.

Below is a modify Dublin Core Schema, and we used an Arabic Vocabulary.

```
<rdf:RDF
Xmlns="http://www.w3.org/TR/1999/PR-rdf-schema-19990303#"
Xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Property rdf:ID="title">
<label  xml:lang="en">title</label>
<SubPropertyOf
          rdf:resource="http://pur1.org/dc/elements/1.1/title" />
</rdf:Property>

<rdf:Property rdf:ID="creator">
<label  xml:lang="en">Author</label>
<SubPropertyOf
           rdf:resource="http://pur1.org/dc/elements/1.1/creator" />
</rdf:Property>

<rdf:Property rdf:ID="subject">
<label  xml:lang="en">Subject</label>
<SubPropertyOf
           rdf:resource="http://pur1.org/dc/elements/1.1/ subject " />
</rdf:Property>

<rdf:Property rdf:ID="description">
<label  xml:lang="en">Description</label>
<SubProbertyOf
           rdf:resource="http://pur1.org/dc/elements/1.1/ description " />
</rdf:Property>

<rdf:Property rdf:ID="publisher">
<label  xml:lang="en">Publisher</label>
```

```
<subPropertyOf
        rdf:resource="http://pur1.org/dc/elements/1.1/ publisher " />
</rdf:Property>

<rdf:Property rdf:ID="date">
<label  xml:lang="en">Date</label>
<subPropertyOf
        rdf:resource="http://purl.org/dc/elements/1.1/date" />
</rdf:Property>

<rdf:Property rdf:ID="type">
<label  xml:lang="en"> type</label>
<subPropertyOf
        rdf:resource="http://purl.org/dc/elements/1.1/type" />
</rdf:Property>

<rdf:Property rdf:ID="format">
<label  xml:lang="en">Format</label>
<subPropertyOf
        rdf:resource="http://purl.org/dc/elements/1.1/format" />
</rdf:Property>

<rdf:Property rdf:ID="rights">
<label  xml:lang="en">Rights</label>
<subPropertyOf
        rdf:resource="http://purl.org/dc/elements/1.1/rights" />
</rdf:Property>

<rdf:Property rdf:ID="language">
<label  xml:lang="en">Language</label>
<subPropertyOf
        rdf:resource="http://purl.org/dc/elements/1.1/language" />
</rdf:Property>

<rdf:Property rdf:ID="keywords">
<label  xml:lang="en">Keywords</label>
<subPropertyOf
        rdf:resource="http://purl.org/dc/elements/1.1/keywords" />
</rdf:Property>

</rdf:RDF>
```

b. Book Schema

The book schema contains the keyword use in the "Subject" property of Dublin Core schema. That property should contain as many of the following keywords as are applicable. It makes a specific statement about a piece of media content.

The key words have the following meaning:

- **Edition**: The edition number of the book.
- **Place**: The geographic Place of publication.
- **Published-Date:** A date associated with the availability of the book.
- **Notes**: Additional information about the book.
- **Institution**: Institution that contributed the book.
- **Abstract:** a brief statement that presents the main points in a concise form.
- **ISBN:** International Standard Book Number.
- **ISSN:** International Standard Serial Number.
- **URL:** If the resource exists online at holding institution, provide the URL.

```
<rdf:RDF
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns"
xmlns="http://www.w3.org/2000/01/rdf-schema#"
xmlns:book="">
<Class rdf:ID="keywords">
<comment xml:lang="en">An enumeration of keywords to describe the subject of
book.</comment>
</Class>
<content:keywords rdf:ID=" Edition">
      <label xml:lang="en"> edition </label>
</content:keywords>
<content:keywords rdf:ID=" Place ">
     <label xml:lang="en">place</label>
</content:keywords>
<content:keywords rdf:ID=" Published-Date ">
     <label xml:lang="en"> published-date </label>
</content:keywords>
<content:keywords rdf:ID="Note">
     <label xml:lang="en">note</label>
</content:keywords>
<content:keywords rdf:ID=" Institution ">
    <label xml:lang="en">institution </label>
</content:keywords>
<content:keywords rdf:ID=" Abstract ">
    <label xml:lang="en"> abstract </label>
</content:keywords>
<content:keywords rdf:ID=" ISBN ">
    <label xml:lang="en"> ISBN </label>
</content:keywords>
<content:keywords rdf:ID=" ISSN ">
    <label xml:lang="en"> ISSN </label>
</content:keywords>
<content:keywords rdf:ID=" URL ">
    <label xml:lang="en"> URL </label>
</content:keywords>
```

5. Example

This example of the metadata in RDF format that is explains the book:

```
<? xml version='1.0' encoding='ISO-8859-1'?>
```

```
<rdf:RDF xmlns:RDF="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:rdfs="http://www.w3.org/TR/1999/PR-rdf-schema-19990303#"
xmlns:pd0= "http://www.w3.org/2000/LibraryRDF/dc-1-0#"
xmlns:pd1= http://www.w3.org/2000/LibraryRDF/technical-1-0#>
<rdf:Description rdf:about="">
   <pd0:Title> Programming Abstractions in C++</pd0:Title>
   <pd0:Creator> Eric S. Roberts</pd0:Creator>
   <pd0:Subject> Programming Abstractions in C++</pd0:Subject>
   <pd0:Description> Bestselling Programming Tutorial and Reference Completely Rewritten for
        the New C++11 Standard.</pd0:Description>
   <pd0:Publisher>Stanford University </pd0:Publisher>
   <pd1:Editor>Stanford University </pd1:Editor>
   <pd0:Publication-Date> 2012</pd0:Publication-Date>
   <pd1:Place > Stanford</pd1:Place>
   <pd1:URL>http://StanfordUnivercity.org </pd1:URL>
   <pd0:Copyrighte> Stanford Univercity </pd0:Copyrighte>
   <pd1:ISBN>001245689 </pd1:ISBN>
   <pd0:Keywords>C++ </pd0:Keywords>
   <pd0:Keywords>Programming</pd0:Keywords>
   <pd0:Keywords>object orented programming </pd0:Keywords>
   <pd0:Keywords>oop </pd0:Keywords>
   <pd0:Format>PDF</pd0:Format>
   <pd0:Language>en</pd0:Language>
 </RDF:Description>
</RDF:RDF>
```

7. Conclusion

In our days people can be refer to the semantic web as the next generation of the WWW. To make an improve to the data aggregation and in order to get precise information from the available information to us. A libraries can play a big role in publishing the knowledge which it make as a huge repository of knowledge,So to provide a more meaningful search in digital libraries we modify and extend the Dublin Core standared Metadata about the bibliographic digital library search.

8. References

1- **Witten**, Ian H., Bainbridge, David Nichols. (2014) **"How to Build a Digital Library "**, ISBN 978-0123748577.
2- **Carrie** Moran, **"The Use of Semantic Web Technologies in Digital Libraries"**, December 5.
3- **Preedip** Balaji B1, Amit Kumar Sarangi1, Devika P. Madalli1. (2012) Knowledge Organization Systems for Semantic Digital Libraries, Documentation Research an Training Centre, Indian Statistical Institute, Bangalore, 10-13.
4- **Bendik** Bygstad, Gheorghita Ghinea, Geir-Tore Klaebo. **Organizational Challenges of The Semantic Web in Digital Libraries**.
5- **National** Information Standards Organization. (2004) Understanding Metadata**.** Niso Press, URL www.niso.org.

6- **Frank** Manola andEric Miller. (2004) RDF Primer, (W3C) Semantic Web Activity Lead, 10-2-2004. URL: http://www.W3C.org/TR/2004/REC-rdf-primer-20040210/.

7- **Jaehoon** Kim, Kangsoo Jung, Seog Park. (2008) An RDF Triple based Acces Authorization Specification Considering Subsumption Relationships, Department of Computer Science, Sogang University, ICDEW 2008. IEEE 24th International Conference.

Analysis flow of second order fluid in a vertical channel with porous wall by using the Homotopy Analysis Method (HAM)

Wala'a Abdul- Mageed Mahdi, Ahmed M. A. Hadi

Department of Programming Engineering, **Madenat Alelem University College**

Malak.rahf@gmail.com

Abstract

In this paper, the state of non newtonian fluid of second order flow injected uniformly into the vertical channel with porous wall through one side of the channel. The equations which are used to describe the flow are the motion and the energy equations. It found that these equations are controlled by many dimensionless numbers such as Reynolds number (Re), Peclet number (Pe), Hartman number (M) and the material of fluid (α, β). The homotopy analysis method (HAM) is used to obtain the analytic solution for the velocity and heat transfer. The effect of each dimensionless parameters upon the velocity and temperature distribution is analyzed and shown graphically by using MATLAB package.

Keywords: Hartman number, Peclet number, vertical channel

المستخلص

ان هذا البحث يتضمن دراسة لجريان مائع لا نيوتيني من الرتبة الثانية في قناة عمودية ذات جدار مثقبة، المعادلات التي استخدمت لوصف حركة المائع هي معادلات الحركة ومعادلة الطاقة وقدحلت تحليلياً باستخدام طريقة الهوموتوبي حيث وجد ان هذه المعادلات تحكمها اعداد لابعدية مثل عدد رينولدز و،بلكت،هارتمان وثوابت اخرى تخص المائع . كماقمنا بدراسة تأثير تلك الاعداد اللابعدية المذكورة .وقدتم استخدام البرنامج الجاهز الماتلاب في هذا البحث .

Intrduction

Fluid is that state of matter, which capable of changing shape and capable of flowing. Fluids may be classified as "Viscous" and "Perfect" according to whether the fluid capable of exerting shearing stress or not. Viscous is called Newtonian if the relation between stress and rate of strain (state of equation) is linear, otherwise is called non – Newtonian fluid .The flow of Newtonian and non – Newtonian fluids in the porous channel has been subject extensive theoretical studies till date because many applications of them in different scientific fields. Examples, of such flow of fluid in vertical porous channel, is found in [11] as the simplest subclass for which one can hope to gain an analytic solution.

The flow of Newtonian and non – Newtonian fluids through porous channel has been investigated by numerous authors. The case of a two dimensional, incompressible, steady, laminar suction flow of Newtonian fluid in a porous channel was studied by Berman [5]. He has solved the Navier-Stokes equations by using a perturbation method for very low cross – flow Reynolds number. After his pioneering work, this problem has been studied by many researchers considering various variations in the problem [7,8].

Wang and Skalak [17] were the first persons who present the solution for a three – dimensional problem of fluid injection through one side of a long vertical channel for Newtonian fluid .They have obtained a series solution for a small value of Reyonlds number and numerical solution for small and large Reynolds number.

Huang [10] re- examined Wang and Skalak problem using a method based upon quasilinearization. Ascher [4], Sharma and Chaudhary [16] reconsidered the above –mentioned problem by introducing a second viscoelastic fluid. They obtained the second order perturbation solution by assuming that the cross– flow of Reynolds number is a small.

Baris [6] continued the last mentioned research by substituting thermodynamically compatible fluid of second grade instead of Newtonian fluid. The used analytical method by Baris was traditional perturbation solution, which was one of old analytical methods.

These scientific problems are modeled by ordinary or partial differential equations and should be solved using special techniques, because in most case, analytical solutions can't be applied to these problems. In resent years, much attention has been devoted to the newly developed methods to constant an analytical solution of these equations. One of these techniques is homotopy Analysis Method (HAM), which was introduced by Liao [14,15] and has been successfully applied to solve many types of nonlinear problems[1,2,11,12]. HAM is a powerful technique for solving linear and nonlinear partial differential equation for example the equation that appears in our problem. In most cases of nonlinear problems can be described by a set of governing linear equations with its initial / boundary conditions [14].

The paper was dependent upon work of Khalid, Ahmed [13]. They are investigated to find the velocity, heat transfer and pressure variation profiles of Newtonian fluid in a vertical channel with porous wall. The governing non- linear problems have been solved analytically by using HAM. In this paper, HAM is employed to find the velocity, heat transfer and pressure variation profiles of non- Newtonian fluid of second order in a vertical channel with porous wall and examine

qualitatively the effect of non –Newtonian parameters (α,β) which are dimensionless numbers, Reynolds number Re, Hartmann number M, and Peclet number Pe on these value .

Governing Equations:

The study of second grad fluid in a vertical channel with porous wall is considered. Fig.1 shows the physical model and coordinate system. A fluid is injected through a vertical porous plate at y=D with uniform velocity U. The fluid strikes another vertical impermeable plate at y=0.It flows out through the opening the plates, due the action of gravity along the Z-axis. The distance between the walls is assumed D, is a small compared to the dimensions of plates, i.e., L $\gg B \gg D$. Due to this assumption the edge effects can be ignored and the isobars are parallel to the Z-axis.

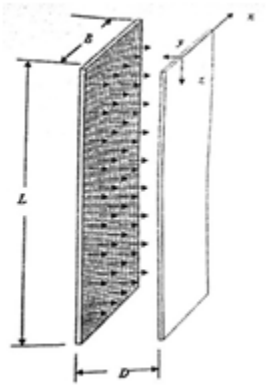


Fig.1Schesh the problem under discussions

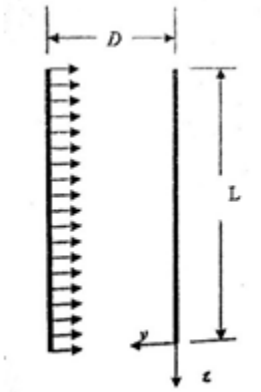


Fig.2 Fluid flow in a vertical channel

The Caushy stress tensor in such a fluid is related to the motion equations in the following manner [9].

T=-PI+$\mu A_1 + \alpha_1 A_2 + \alpha_2 {A_1}^2$
(1)

where $A_1 = \nabla \boldsymbol{V} + (\nabla \boldsymbol{V})^T$

$$A_2 = \frac{dA_1}{dt} + A_1(\nabla \boldsymbol{V}) + (\nabla \boldsymbol{V})^T A_1 \qquad (2)$$

$$\mu \geq 0, \qquad \alpha_1 \geq 0, \alpha_2 \geq 0 \qquad (3)$$

In this equation, P is the pressure, $\boldsymbol{V}$ is the velocity vector, ∇ is the gradient oparoter, $\alpha_i (i = 1,2)$ are the material moduli of fluid, d/dt is the material derivative and $A_i (i = 1,2)$ are the two first Rivilin Eriksen tensor.

Note that for α_1, α_2=0 equation (1) along with (2) descries of Newtonian fluid [13]. In addition to (1) the basic equations of the problem are in the following:

$$\nabla \boldsymbol{V} = 0 \qquad (4)$$

$$\rho(\boldsymbol{V}\nabla \boldsymbol{V}) = \nabla T + (\boldsymbol{J} \times \boldsymbol{B}) \qquad (5)$$

$$\rho Cp(\mathbf{V}\nabla T) = K\Delta T \quad (6)$$

Equations (4), (5) and (6) are the continuity, momentum and energy equations, respectively. Where ρ is the density and ($\mathbf{J}\times \boldsymbol{B}$) is Lorenz force vector. The fluid is assumed to be steady and laminar. Substituting the stress tensor T from (1) into (5) yields:

$$\rho(\boldsymbol{V}\nabla V) = -\nabla P + \mu(\nabla^2 \boldsymbol{V}) - \sigma u B^2 \quad (7)$$

The velocity components corresponding to X ,Y ,Z direction respectively denoted by u ,v ,w, following [17] , we look for a solution, compatible with the continuity of the form :

$$u= \frac{Ux}{D} f'(\eta) \quad ,v =-Uf(\eta) \quad , \quad w=\frac{D^2 g\rho}{\mu} h(\eta) \quad (8)$$

where $\eta = y/D$ and the prime denoted the differential with respect to η .

The boundary conditions for the velocity field are :

$$f(0)=0 \quad , \quad f(1)=1 \quad f'(0)=0, \quad f'(1)=0, \quad f''(0)=6 \quad (9)$$

It follows from (7) and equation of motion that :

$$\frac{\partial P}{\partial x} = \frac{Ux}{D^2}[Re(ff'' - f'^2) + f'''' - Mf' + \alpha\left(-ff'''' + 2f'f''' + 3f''^2\right) + \beta(2f''^2)] \quad (10)$$

$$\frac{\partial P}{\partial \eta} = -Reff' - \frac{\mu U}{D}[f'' + \alpha\left(ff''' + 6f'f'' + \frac{8x^2}{D^2} f''f'''\right) + \beta\left(8f'f'' + \frac{2x^2}{D^2} f''f'''\right)] \quad (11)$$

Where the cross –flow Reynolds number ,Re, M is the Hartmann number, and α,β are the dimensionless numbers ,are defined through respectively.

$$Re= \frac{\rho UD}{\mu} \quad , \quad M= \frac{\sigma uB}{\mu} \quad , \quad \alpha = \frac{U\alpha_1}{\mu D} \quad , \quad \beta= \frac{U\alpha_2}{\mu D} \quad (12)$$

Integrating (11) with respect to η ,obtained equation is:

$$P(x, \eta) = -\frac{1}{2} f^2 + \frac{\mu U}{D}\left[-f' + \alpha\left(ff'' + \frac{5}{2} f'^2 + \frac{4x^2}{D^2} f''^2\right) + \beta\left(\frac{x^2}{D^2} f''^2 + 4f'^2\right)\right] + \varphi(x) \quad (13)$$

Where $\varphi(x)$ is arbitrary function of x. different ion of the above equation with respect to x yields:

$$\frac{\partial P}{\partial x} = \frac{\mu U}{D}\left[\frac{8x}{D^2}\alpha f''^2 + \frac{2x}{D^2}\beta f''^2\right] + \frac{d\varphi}{dx} \quad (14)$$

Combining of (14) and (10)

$\frac{d\varphi}{dx} = \frac{\mu Ux}{D^3}[Re(ff'' - f'^2) + f'''' - Mf' + \alpha(-ff'''' + 2f'f''' + 3f''^2) + \beta(2f''^2)] - \frac{\mu U}{D}\left[\frac{8x}{D^2}\alpha f''^2 + \frac{2x}{D^2}\beta f''^2\right]$ (15)

And

$\frac{D^3}{\mu Ux}\frac{d\varphi}{dx} = [Re(ff'' - f'^2) + f'''' - Mf' + \alpha(-ff'''' + 2f'f''' - 5f''^2)$ (16)

It is apparent that the quantity in parentheses in (16) must be independent of η.Hence ,the following equation for f is:

$f'''' + Re(ff'' - f'^2) - Mf' + \alpha(-ff'''' + 2f'f''' - 5f''^2) = C$ (17)

Where C arbitrary constant which takes value

$C = f''''(0)$ (18)

Now differentiating (17) with respect to η yields :

$f''''' + Re(f'''f - f'f'') - Mf'' + \alpha(-ff''''' + f'f'''' - 8f''f''')$ (19)

by using (17) ,$\varphi(x)$ can be written as

$\varphi(x) = \frac{\mu Ux^2}{2D^3}C + C_0$ (20)

Where C_0 is the constant of integration. Inserting $\varphi(x)$ from (20) into (13) :

$P(x,\eta) = -\frac{1}{2}f^2 + \frac{\mu U}{D}\left[-f' + \alpha\left(ff'' + \frac{5}{2}f'^2 + \frac{4x^2}{D^2}f''^2\right) + \beta\left(\frac{x^2}{D^2}f''^2 + 4f'^2\right)\right] + \frac{\mu Ux^2}{2D^3}C + C_0$ (21)

from (21) ,the pressure variation in x and y direction can be written in dimensional form as follows:

$P(x) = \frac{P(0,\eta) - p(x,\eta)}{\rho U^2} = -\frac{1}{Re}(4\alpha f''^2 + \beta f''^2 + \frac{1}{2}f''''(0))(\frac{x}{D})^2$ (22)

$P(y) = \frac{P(x,0) - p(x,\eta)}{\rho U^2} = \frac{f^2}{2} + \frac{1}{Re}(f' + \alpha(ff'' + \frac{5}{2}f'^2) + 4\beta f'^2)$ (23)

Note that the equations (10),(11),(13),(15),(16),(17),(19) and (21) becomes in Newtonian flow [13] where we put α and $\beta = 0$.

Equations for Temperature 3- Governing

In this section ,temperature field as below

$T = T_0 + (T_1 - T_0)\theta(\eta)$ (24)

where T_0, T_1 are the temperatures of impermeable and porous plates, respectively and with constant value . Substituting(8)and(24)into (6) lead to the following equation:

$$\theta'' + Pe\theta' = 0 \qquad (25)$$

where Pe $=\rho UDcp/k$ is the Peclet number .Equation (25) is solved subject to the boundary conditions

$$\theta(0) = 0\,, \quad \theta(1) = 1 \qquad (26)$$

4- Solution Using Homotopy Analysis Method

In this section HAM is applied to solve (19) subject to the boundary conditions (9) .The initial guesses and linear operators are chosen in the following :

$$f_0(\eta) = 3\eta^2 - 2\eta^3 \qquad (27)$$

As the initial guess approximation for $f(\eta)$ is

$$L_1(f) = f^v \qquad (28)$$

As the auxiliary linear operator has the property:

$$L(c_1 + c_2\eta + c_3\eta^2 + c_4\eta^3 + c_5\eta^5) = 0 \qquad (29)$$

And $c_i(i = 1 - 5)$ are constant. Let p∈ [0,1]denotes the embedding parameter and h indicates non zero auxiliary parameters .Then the following equation are constructed:

$$(1-p)L_1(f(\eta;p) - f_0(\ \eta)] = ph_1N_1[f(\eta;p)] \qquad (30)$$

$$f(0;p) = 0, f'(0;p) = 0\ , f(1;p) = 1, f'(1;p) = 1 \qquad (31)$$

$$N_1[f(\eta;p)] = f''''(\eta;p) + Re\big(f'''(\eta;p)f(\eta;p) - f'(\eta;p)f''(\eta;p)\big) - Mf''(\eta;p) + \alpha(-f(\eta;p)f'''''(\eta;p) + f'(\eta;p)f''''(\eta;p) - 8f''(\eta;p)f'''(\eta;p)) = 0 \qquad (32)$$

for p=0 and p=1:

$$f(\eta;p) = f_0(\eta), \quad f(\eta;1) = f(\eta) \qquad (33)$$

When p increases from 0 to 1 then $f(\eta;p)$vary form $f_0(\eta)$ to $f(\eta)$.By using Taylor's theorem and using (33):

$$f(\eta;p) = f_0(\eta) + \sum_{m-1}^{\infty} f_m(\eta)p^m, f_m(\eta) = \frac{1}{m!}\frac{\partial^m(f(\eta;p))}{\partial p^m} \qquad (34)$$

$$f(\eta) = f_0(\eta) + \sum_{m-1}^{\infty} f_m(\eta) \qquad (35)$$

The $mth-$ order deformation equations are:

$$L[(f_m(\eta) - X_m f_{m-1}(\eta)] = hR^f{}_m(\eta), \quad (36)$$

The boundary conditions are:

$$f_m(0) = f'_m(0) = f_m(1) = f'_m(1) = 0 \quad , f''_m(0) = 6 \quad (37)$$

Where $R^f{}_m(\eta) = f''''_m + \mathrm{Re}\sum_{i=0}^{m-1}(f_{m-1}f'''_i - f'_{m-1}f''_i) - Mf''_{m-1} + \alpha(\sum_{i=0}^{m-1}(-f_{m-1}f'''''_i + f'_{m-1}f''''_i - 8f''_{m-1}f'''_i))$ (38)

$$X_m = \begin{cases} 0 & m \le 1 \\ 1 & m > 1 \end{cases} \quad (39)$$

To find the solution of m th -order deformation ,we shall use the symbolic software MATLAB up to first few order of approximation . We found the solution up to 3 th order approximation and they are:

$f_1 =$

$24Reh\eta^3 - \eta^4((Mh)/4 - 24\alpha h) - \eta^5((Mh/20) - (24\alpha h)/5) - \eta^3(Mh - 96\alpha h) - \eta^2(3Mh - 288\alpha h) - \eta^4((3Reh)/2 - (Mh)/2 + 48\alpha h) - \eta^5((3Reh/10 - (Mh)/10 + (48\alpha h)/5) - \eta^6(Reh)/20 - (Mh)/60 + (8\alpha h)/5) - \eta^3(6Reh - 2Mh + 129\alpha h) - \eta^2(18Reh - 6Mh + 576\alpha h) - \eta(6Mh - 576\alpha h) - 6Reh\eta^4 - (6Reh\eta^5)/5 - (Reh\eta^6)/5 - (Reh\eta^7)/35 - (Reh\eta^8)/140$

$f_2 =$

$(37Re^2h^2\eta^9)/210 - \eta^8((6Re^2h^2)/35 - (MReh^2)/140 + (183Re\alpha h^2)/35) - \eta^9((Re^2h^2)/28 - (MReh^2)/504 + (67Re\alpha h^2)/210) - \eta^6(18Re^2h^2 - MReh^2 + (804Re\alpha h^2)/5) - \eta^7((18Re^2h^2)/7 - (MReh^2)/7 + (804Re\alpha h^2)/35)\ldots\ldots\ldots\ldots\ldots$

$f_3 =$

$\eta^{16}((181Re^3h^3)/100900800 + (MRe^2h^3)/42042000 + (11Re^2\alpha h^3)/1092000) - \eta^8((9Re^2h^2)/28 - (MReh^2)/56 + (201Re\alpha h^2)/70) - \eta^8((6Re^2h^2)/35 - (MReh^2)/140 + (1831Re\alpha h^2)/35) - \eta^9((Re^2h^2)/28 - (MReh^2)/504 + (67Re\alpha h^2)/210) - \ldots\ldots\ldots$

5- Convergence of Solution (4)

We notice that the explicit analytical expression in eq.(34) contain the auxiliary parameter h_1.As pointed out by Liao [14] ,the convergence region and the rate of approximations given by the HAM are strongly depending on h_1.. By means of so-called h-curve for the velocity profile figure (3). The range of admissible value of $h_1$for the velocity profile when Re=10, M=1, and $\alpha = 1$ is $-1.8 \ge h_1 \ge -0.2$. Note that if $\alpha = 0$, then the series belong in [13].

6-Solution of Energy Equation

In this section HAM is applied to solve (25) subject to the boundary conditions (26) The initial guesses and linear operators are chosen in the following:

$$\theta(\eta) = \eta \quad (40)$$

As the initial guess approximation for $\theta(\eta)$ is

$L_2(\theta) = \theta''$ (41)

As the auxiliary linear operator has the property:

$L(c_1 + c_2\eta) = 0$ (42)

And $c_i(i = 1 - 2)$ are constant. Let p∈ [0,1]denotes the embedding parameter and h indicates non zero auxiliary parameters .Then the following equation are constructed:

Zeroth − order deformation equations

$(1 - p)L_1(\theta(\eta; p) - \theta_0(\ \eta)] = ph_2N_2[\theta(\eta; p)]$ (43)

$\theta(0;p) = 0, \qquad \theta(1; p) = 1$ (44)

$N_2[\theta(\eta; p)] = \theta''(\eta; p) + Pe\big(f(\eta; p)\theta'(\eta; p)\big)=0$ (45)

for p=0 and p=1:

$\theta(\eta; 0) = \theta_0(\eta), \theta(\eta;1) = \theta(\eta)$ (46)

When p increases from 0 to 1 then $\theta(\eta; p)$vary form $\theta_0(\eta)$ to $\theta(\eta)$.By using Taylor's theorem and using (46):

$\theta(\eta; p) = \theta_0(\eta) + \sum_{m-1}^{\infty}\theta_m(\eta)p^m,\ \theta_m(\eta) = \frac{1}{m!}\frac{\partial^m(\theta(\eta;p))}{\partial p^m}$ (47)

$\theta(\eta) = \theta_0(\eta) + \sum_{m-1}^{\infty}\theta_m(\eta)$ (48)

The mth − order deformation equations

$L[(\theta_m(\eta) - X_m\theta_{m-1}(\eta)] = hR^{\theta}{}_m(\eta),$ (49) The boundary conditions are:

$\theta_m(0) = \theta_m(1) = 0$ (50)

Where $R^{\theta}{}_m(\eta) = \theta''{}_{m-1}$+Pe$\sum_{i=0}^{m-1}(f_{m-1}\theta'_i)$ (51)

$X_m = \begin{cases} 0 & m \le 1 \\ 1 & m > 1 \end{cases}$ (52)

To find the solution of m th -order deformation ,we shall use the symbolic software MATLAB up to first few order of approximation . we found the solution up to 3 rd. order approximation and they are:

$\theta_1 =$

$-(Peh\eta^4(2\eta - 5))/20 - (Peh\eta^3(\eta - 2))/2$

$\theta_2 =$

$\eta^8((Pe^2h^2)/8-(RePeh^2)/280-\eta^2(3MPeh^2-288Pe\alpha h^2)-\eta^3((\mathrm{MPe}h^2-96Pe\alpha h^2)+\eta^9((Pe^2h^2)/72-(RePeh^2)/2520)+\eta^5((9Pe^2h^2)/5+(MPeh^2)/20-(3PeReh^2)/2-(24Pe\alpha h^2)/5)-\eta^6((3Pe^2h^2)/120-(MPeh^2)/20+(PeReh^2)/4+(4Pe\alpha h^2)/5)+\eta^6((3Pe^2h^2)/10+(MPeh^2)/120-(PeReh^2)/4-(4Pe\alpha h^2)/5)-\cdots\ldots\ldots\ldots\ldots\ldots\ldots$

$\theta_3 =$

$\eta^8((Pe^2h^2)/8-(RePeh^2)/280-\eta^2((3MPeh^2-288\alpha Peh^2)-\eta^2(3MPeh^3-288\mathrm{Pe}\alpha h^3)-\eta^3(MPeh^2-96Pe\alpha h^2)+\eta^9((Pe^2h^2)/72-(RePeh^2)/2520)-\eta^7((M^2Peh^3)/168+(17MPe^2h^3)/28-(5MPeReh^3)/14-(17MPe\alpha h^3)/7)-\cdots\ldots\ldots\ldots\ldots$

7-Convergence of Solution (6)

The explicit analytical expression in eq.(47) contain the auxiliary parameter h_2.As pointed out by Liao [14] ,the convergence region and the rate of approximations given by the HAM are strongly depending on h_2.. By means of so-called h-curve for the temperature profile figure (4). The range of admissible value of $h_2$for the temperature profile when Re=10, M=1, and $\alpha = 1$ is $-1.8 \geq h_2 \geq -0.2$,note that if $\alpha = 0$, then the series belong in [13].

8-Results analysis

In this section, we studied the effect of dimensionless parameters that governing the momentum and energy equations, upon the normal, tangential velocities and temperature of vesicant fluid of second order in a vertical channel. All results are plotted by MATLAB package. Figures (5,6) shows the effect of Hartmann number M on the normal and the tangential velocity components (η), we keep Re=10,$\alpha = 1$ and M has been given 0.001,1,5 and 15. The following results are observed: As Hartmann M increases, there is a small decreasing in normal and tangential velocity component range. Figure 7 shows the function which correspond to the velocity components have been plotted versus η for Re=1,10,20 fixed M=1,and $\alpha = 1$. For increase values of Reynolds number then the velocity increasing.

Figure 9 illustrates the effect of dimensionless parameter α on the normal velocity profiles for fixed Re=10,M=1 and α=0.002,2,4.5.It obvious from this this figure that the effect of α is very strong on the normal velocity profile where it increases, and if we put α =0,then the velocity profile becomes in flow of Newtonian fluid cases[13].

Figure 10 depicts the tangential velocity for Re=10,M=1 and $\alpha = 1,3,4.5$. It is obvious for this figure that the tangential velocity increases if the value of α is large.

Figures 11 and 12, the effects of section and injection have been investigated, as it showed by contours.

Figure 15 depicts the profiles of temperature in viscoelastic fluid in a vertical channel with porous wall .when Re=10,M=1, α =1 that the effect of Peclet number on temperature profile was shown. According to definition of Peclet number was increased of uniform injection velocity. Due the convection effects, increasing of Peclet number led to intensity the temperature distribution in the channel. Figure 13 and 14 present the pressure variations in x and y directions, respectively when Re=10,M=1. From the evident the pressure variations will increase with increasing of non - Newtonian parameters α andβ.

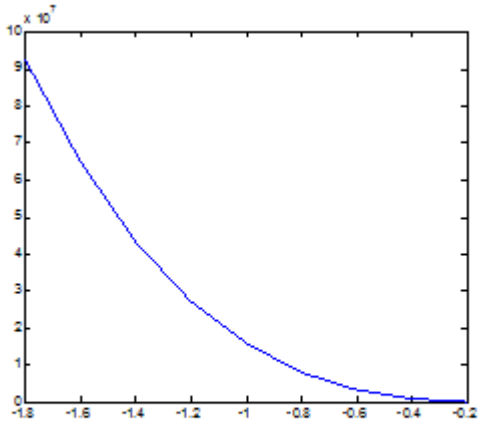


Fig.3 The h_1 curve for Re=10,M=1,α=1

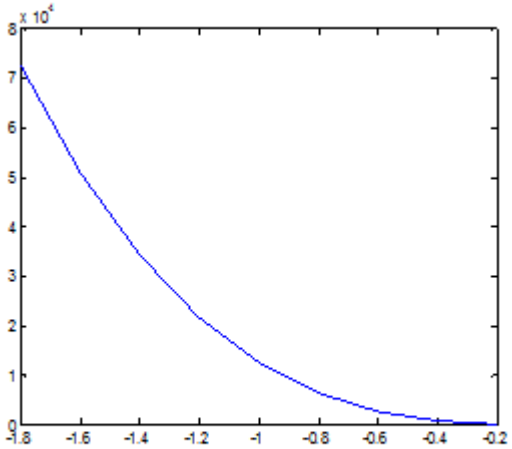


Fig.4 The h_2 curve for Re=10,M=1,α=1,Pe=1

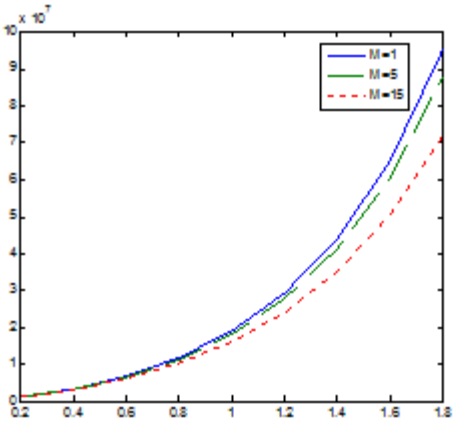


Fig.5 The velocity for Re=10,α = 1

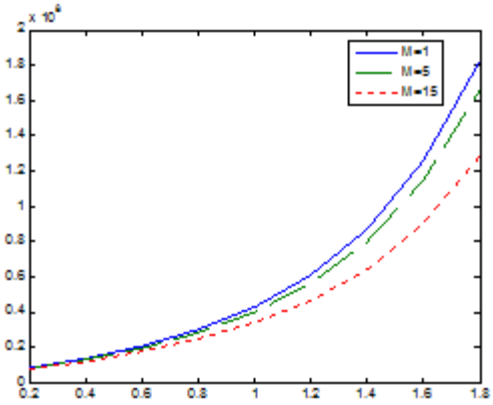


Fig.6 The tangential velocity for Re=10,α = 1

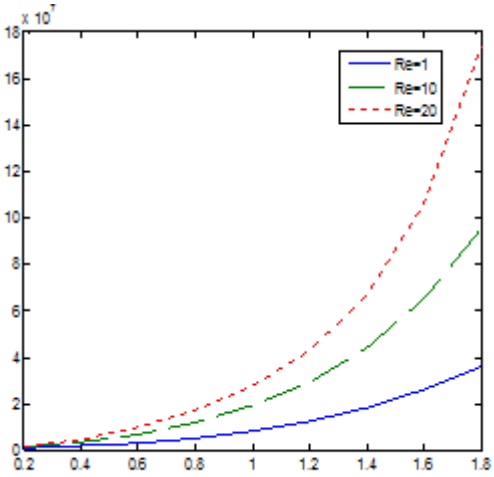


Fig7 The velocity for M=1 ,$\alpha = 1$

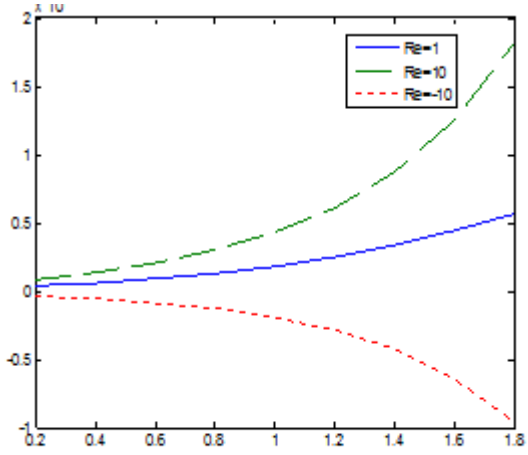


Fig.8 The tangential velocity for M=1 ,$\alpha = 1$

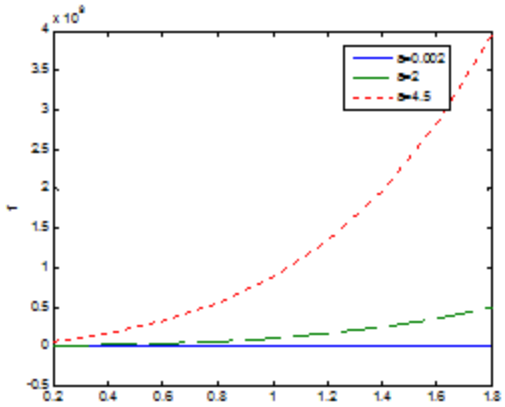


Fig.9 The velocity for M=1 ,$Re = 10$

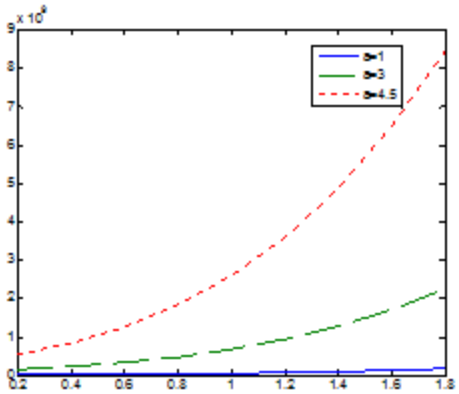
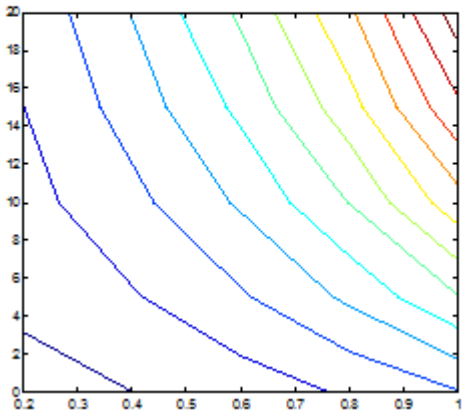


Fig10 The tangential al velocity for M=1 ,Re=10



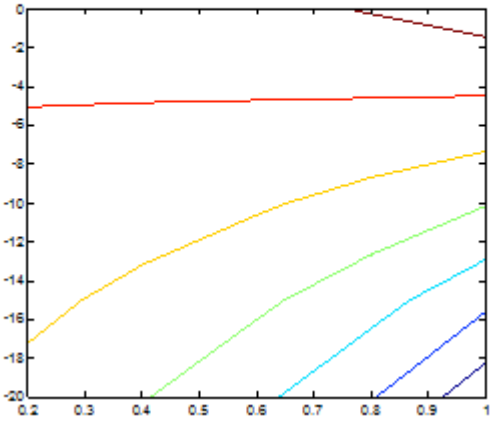
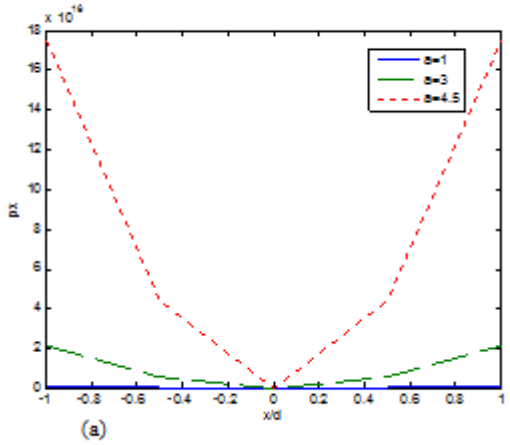
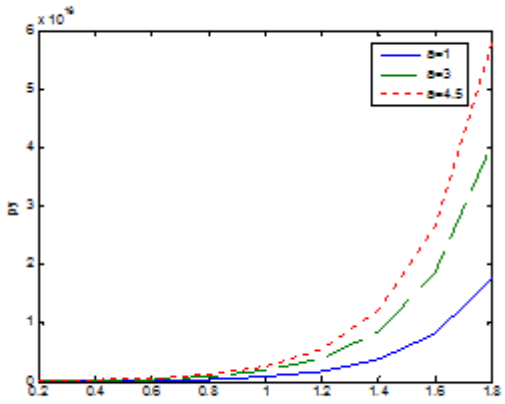


Fig.11The tangential velocity contour for,$Re = 10$



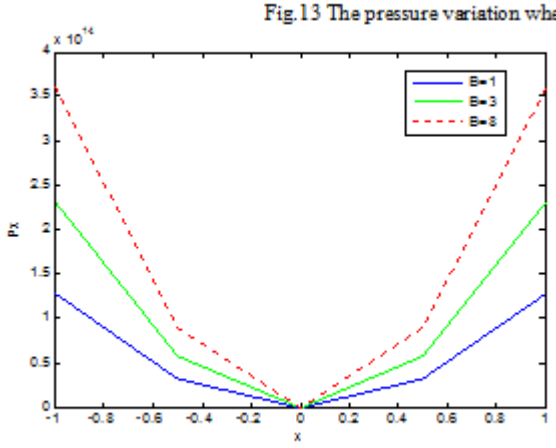
(a)

Fig.12 The tangential velocity contour for,$Re = -10$

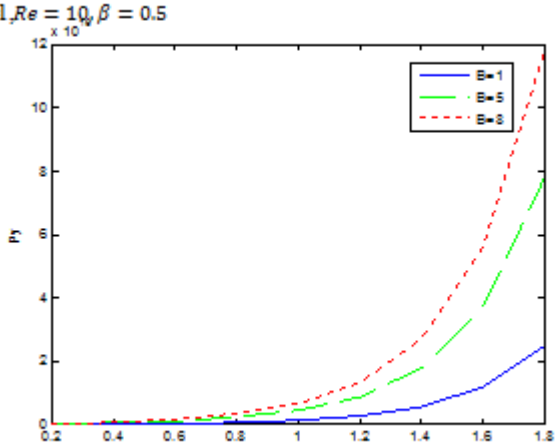


(b)

Fig.13 The pressure variation when M=1,$Re = 10, \beta = 0.5$



(a)



(b)

Fig.14 The pressure variation when M=1,$Re = 10, \alpha = 1$

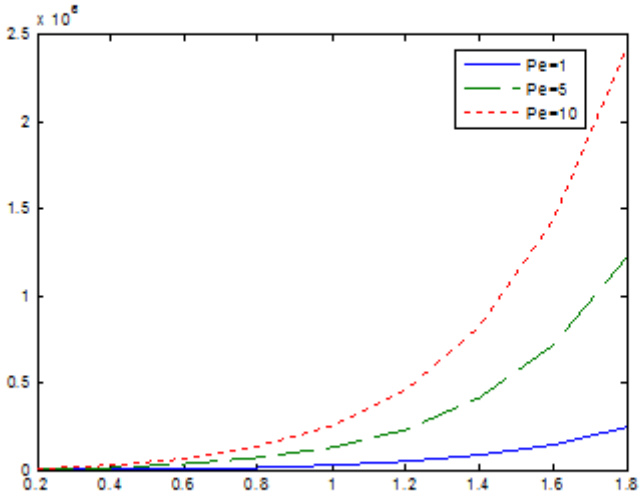


Fig.15The temperature variation when M=1,$Re = 10, \alpha$ =1

References

1. **Abbasbandy** S. (2007) The application of homotopy analysis method to solve a generalized Hirota-Satsuma coupled **KdV** equation". Phys .Lett. A. Vol.6.pp.478-483.
2. **Abbasbandy** S. (2008) Solution solutions for the Fitzhugh-Naagumo equation with homotopy analysis method. Appl. Math. Model 32, Vol. 12 , pp. 2706-2714.
3. **Anderas** A . (2001), " Principlle of fluid mechanics ", Printice-Hill, Inc.
4. **Ascher** U ,(1980), "Solving boundary value problems with a sspline-collocation code". J. Comput . Phys. Vol. 34, pp.401-413.
5. **Berman** A.S. (1953) , " Laminar flow in channels with porous walls", J. Appl. Phys. ,Vol.24,pp.1232-1235.
6. **Baris** S. (2001), "Injection of a Non-Newtonian fluid through one side of along vertical channel" . Acta. Mech. Vol.151,pp. 163-170.
7. **Choi** J. J., Rusak Z . , Tichy J. A .(1999), " Maxwell fluid suction flow in a channel ". J. Non-Newtonian Fluid Mwch. Vol.85,pp.165-187.
8. **Cox** S. M. (1991), Two dimensional flow of viscous fluid in a channel with porous walls ". J. Fluid Mech. Vol. 227,pp. 1-33.
9. **Fosdick** R.L., Rajagopal ,K. R. (1980), "Thermodynamic and stability of fluids ". Proc.R. Soc. London. A339-351.
10. **Huang** C. L. (1978), "Aplllication on quasilinearization technique to the vertical channel flow and heat convection ". Int. J. Non-linear Mech., Vol.13, pp.55-60.
11. **Joneidi** A. A. , Bomairry G. , Babaelahi M.(2010),"Homotopy analysis method to Walter's B fluid in a vertical channel with porous wall ". Meccanica Vol.45,pp.857-868.
12. **Hayat** T. , Khan M. , Ayub M. (2004), "On the explicit analytic solutions of an Oldroyd 6 – constant fluid with magnetic field " .J. Eng. Sci. Vlo.42,pp.123-135.
13. **Khalid** I. J. Al-Zaidee ,Ahmed M. A. Hadi , (2013)," The influence of magentodrodynamic Newtonian fluid flow in a vertical channel with porous wall using homotopy analysis method" . College of Science. University of Baghdad.
14. **Liao** S. J (1992) ,'The prposed homotopy analysis technique for solution of nonlinear problems ". PhD thesis ,Shanghai Jiao Tong University .
15. **Liao** S. J (2004), " On the homotopy analysis method for non linear problems ".Appl.Math.Comput., Vol.147,pp.499-513.
16. **Sharma** P. R. , Chaudhar R. C.(1982),"Fluid injection of a Rivilin-Ericksen fluid through one side of a long vertical channel ".Bull.Tech.Univ..Istanbul,Vol.35,pp.401-
17. **Wang** C. Y. ,Skalak F. (1974),"Fluid injection through one side of a long vertical channel". AI ChE J. Vol.20,pp.603-605.

JOURNAL OF MADENT ALELEM COLLEGE VOL 7 NO 2 YEAR 2015

Design and Implementation of A New Hybrid Encryption Algorithm

Ghada Salim Mohamed

Debt.Programing Eng

University Collage Of Madenat Al -Elem

gha_2090@yahoo.com

Abstract

Several approaches and techniques have been proposed to make communication via the Internet secure; one of these approaches is cryptography. In this paper the proposed algorithm based on merge of two encryption algorithms(public key algorithms), also used (XOR logic operation), (NOT logic operation) and permutation operation .The proposed hybrid algorithm consist of many level of cryptography so it has complexity with speed of implementation more than original algorithms.

Key words: Internet, cryptography, logic operation

تصميم وتنفيذ خوارزمية تشفير هجينة جديدة

غادة سالم محمد

كلية مدينة العلم الجامعة

الخلاصة

العديد من التقنيات والطرق اقترحت لجعل الاتصالات عبر الانترنت أمينة . واحدة من هذه الطرق هي التشفير. في هذا البحث تم اقتراح طريقة للتشفير تعتمد على دمج طريقتين من طرق التشفير باستخدام المفتاح المعلن بالإضافة إلى مستويات عديدة من التشفير تعتمد على استخدام (XOR Logic Operation, Not Logic Operation, Permutation Operation. بالتالي فان النظام المقترح يمتلك تعقيد مع سرعة في التنفيذ اكبر من الخوارزميات الأصلية.

1.Introduction

Computers are now found in every layer society, and information is being communicated and processed automatically on a large scale [1]. So that, daily communications of all kinds over the internet have become incredibly popular. Since the rise of the internet, one of the most important factors of information technology and communication has been the security of information. Thus many applications are Internet-based and in some cases, it is desired that the communication be made secret. In essence, the internet is an open channel and security problems such as interception, modification and others are very real.

Several approaches have been proposed to make communication via the internet secure [2]. One of these approaches is Cryptography, where the sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key [3].

Cryptography is the science of writing in secret code [2] and is an ancient art of ensuring that messages (writing) are kept secure (hidden) from those recipients to whom the messages are not addressed [3].

2.Cryptographic Goals

Cryptography is also used to provide solutions for many problems such as:

1.Confidentiality (privacy).

2.Data integrity.

3.Authentication.

4. Non-repudiation.[4]

3.Types of Cryptography

There are several ways of classifying cryptographic algorithms. There are, in general, two types of cryptographic schemes:

a) **Secret Key Cryptography (SKC).**

b) **Public Key Cryptography (PKC).**

3.1 .Secret Key Cryptography (SKC)

It uses a single key for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption [2].

3.2 .Public Key Cryptography (PKC)

Public-key cryptography is considered the most significant new development in cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975. Generic Public-key cryptography (PKC) employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key [4]. One of the keys (public key) is used to encrypt the plaintext and may be advertised as widely as the owner wants. The other key (private key) is used to decrypt the cipher text and is never revealed to another party. The sender encrypts some information using the receiver public key; the receiver decrypts the cipher text using his private key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information [5].

4. Public-Key cryptography algorithms

Public-key cryptography algorithms that are in use today for key exchange or digital signatures include: RSA, Rabin, ElGamal, Paillier, Elliptic Curve Cryptography (ECC),Cramer-Shoup and many other public key cryptography algorithms [5].

4.1 .Rivest, Shamir and Adleman(RSA) Public Key Cryptography

The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L. Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization any other public key cryptography algorithms [5].

4.1.1. RSA keys generation.[3]

The first step in RSA encryption is to generate a key pair. Two keys are generated of which one is used as the public key and the other is used as the private key. The keys are generated with the help of two large prime

numbers. The keys are generated as follows:

Algorithm (1):RSA Initialization.

Input: Two large prime numbers(p,q)

Output: A public keys (n, e), and a private keys (n,d).

1. **Begin.**
2. Generate two large random primes**p** and **q**.
3. Compute n which is equal to product of those two prime numbers,

n= p.q

4. Compute **φ(n) = (p-1)(q-1).**
5. Choose an integer **e, 1 < e <φ(n),** such that **gcd(e, φ(n)) = 1**.
6. Compute the secret exponent **d, 1 < d <φ(n),** such that

e.d ≡ 1 (mod φ(n)).

7. The public key is (n, e) and the private key is (n, d). The values of p,

q, and φ(n) should also be kept secret.

8.End.

- **n** is known as the modulus.
- **e** is known as the public exponent or encryption exponent.
- **d** is known as the secret exponent or decryption exponent.

4.1.2 . RSAEncryption

Encryption is done using the public key component e and the modulus n.

To whomever we need to send the message, we encrypt the messagewith their public key **(e, n).**Encryption is done by taking an exponentiation of the message m withthe public key e and then taking a modulus of it.

Algorithm (2):RSAEncryption

Input: The plaintext to encrypt, the public key (n, e).

Output: The encrypted cipher text.

1. **Begin.**
2. Obtain the recipient's public key**(n,e)**
3. Represent the plaintext message as a positive integer **m < n**
4. Compute the cipher text **c = m^e mod n**.
5. Send the cipher text c to the recipient.
6. **End.**

4.1.3 RSADecryption

Decryption is done using the Private key. The person who is receiving the encrypted message uses his own private key to decrypt the message. Decryption is similar to the encryption except that the keys used are different.

Algorithm (3): (RSA Decryption)

Input: The received encrypted cipher text and the private key.

Output: The original plaintext.

1. **Begin.**
2. Recipient uses his private key **(n, d)** to compute $\mathbf{m = c^{d} \bmod n}$.
3. Extract the plaintext from the integer representative **m**.
4. **End.**

- The RSA algorithm has been implemented in many applications and it is currently one of the most popularly used encryption algorithm [3].

4.2 .Paillier Public Key Cryptography

The Paillier cryptosystem is a probabilistic asymmetric algorithm for public key cryptography, invented by Pascal Paillier in 1999 [6].This probabilistic scheme has generated a good amount of interest, the main interest seems to be centered around the homomorphic property allows this scheme to do simple addition operations on several encrypted values and obtain the encrypted sum. The encrypted sum can later be decrypted without ever knowing the values that made up the sum**.**

The problem of computing n-the residue classes is believed to be computationally difficult. This is known as the Composite Residuosity (CR) assumption upon which this cryptosystem is based , Because of this useful characteristic, the scheme has been suggested for use in the design of voting protocols, threshold cryptosystems, watermarking, secret sharing schemes, private information retrieval, and server-aided polynomial evaluation[7].

4.2.1 .Algorithm (1): Paillier Initialization[6].

Input: Two large prime numbers(**p,q**)

Output: A public keys (**n, g**), and a private keys (**p, q, μ, λ**).

1. **Begin**
2. Select two large prime numbers, p and q about the same size.

3.Compute the modulus n the product of two primes **n =(p*q)** and**λ = LCM (p - 1, q - 1)** (**λ** is Carmichael's function)

(**LCM** is a Least Common Multiplicative)

4. Select random integer**g** where **g** ∈ $Z^*_{n^2}$where g's order being a non zero multiple of n (Since **g = (1 + n)** works and is easily calculated, this is the best choice). This can done efficiently by checking **gcd (L (g mod n^2),n)**=1

5.Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: **μ=L (g∈mod n^2) $^{-1}$mod n** where **function L** is defined as **(Lagrange function) L(u)=u-1\ n for u =1 mod n**

6.Publish the public key **(n, g)** and keep the private key (**p,q, μ, λ**)secret **7.End.**

4.2.2 .Algorithm (2) :(Paillier Encryption)[6].

Input: The plaintext to encrypt, the public key (**n,g**).

Output: The encrypted cipher text.

1. **Begin**
2. Plaintext is m where **m < n**.
3. Find a random r**, r∈ Z^*_n**
4. Compute cipher text **c = g^m .r^n mod n^2.**
5. **End**

4.2.3 .Algorithm (3): (Paillier Decryption) [7]

Input: The received encrypted cipher text and the private key.

Output: The original plaintext.

- **Begin**
- The cipher text **c < n^2**.
- Calculate**α**, where **α.n≡ 1 mod∅(*n*).**
- Retrieve plaintext by compute **m = L(c · r^{-n} mod n^2).**
- **End**

4.2.4 .Paillier Implementation Requirements

There are some of algorithms and definitions [8,9] are used in execution of the Paillier cryptography method that are shown below:

1. Algorithms of (the greatest command divisor (gcd(a,b))):

this algorithm take **a** and **n** positive integer, not equal zero and give as output the largest divisor d such that **d | a** and **d | b**

2. Algorithms of (Inverse (a, n)):

This algorithm take **a** and **n** integer number, and return x such that:

a.xmod **n** =1, where **0 < a < n**.

3. Algorithms of (Fast modular exponentiation):

this algorithm take **x, e** and **n** integer number, and compute the modular exponentiation : $\mathbf{c= x^{e}}$**.**

4. Calculate the modulus (that take **b** and **n** positive integer, not equal zero and give **a** as congruent of **b** modulo **n** where(**b, n, a**) are integer numbers where **0 < a < n.**

5. Other ways that used to increase the performance:

a) Precompute the value $\mathbf{r^n}$ only once in initialization for each message passed.

b) Set **g = (1 + n).** This is the simplest value and there seems to be no benefit of calculating something more complicated.

c) Precompute $\mathbf{n^2}$**,** which is necessary in computing modules $\mathbf{n^2}$**.**

5.Proposed Hybrid-Encryption System

Action Steps of the proposed system could be clarified as follows:

5 .1 The proposed algorithm encryption process

Input: Plain text, Keys.

Output: The cipher text(String of binary bits).

1. **Begin.**
2. Divided the plain text (PT) into blocks (bi) each one consist of 8 characters, process one block each time.
3. Convert the characters of block to decimal form by using ASCII code .

4. Encryption the decimal number by using **The Proposed Hybrid Public Key Method(Algorithm(A),(Algorithm(B)).**
5. Divide the result cipher number by 256 , store the result of division in D1,and store the remainder of division in D2
6. Convert D1 to string of bits(S1),Convert D2 to string of bits(S2).
   (we can use **n** instead of 256 ,the difference will be in number of bits that used to represent result cipher number form ,**The length of binary string of bits=2* Number of bits used to represent n in binary form**)
7. Perform (S1 XOR S2)that give S3
8. Concatenate S1 and S3 in one string (S4)
9. Perform NOT (S4) that give string (S5).
10. Reverse the order of bits of S5
11. Perform ((new S5) XOR (String of bits S6(S6=the secret key **d** in binary form)).
12. Store the bits of string into 2D array (4X4) and Permutation the elements of the array depend on specific 2D array (4x4) that shown in **Figure(2).**
13. Convert the permuted array element into one string of 16 bits.
14. Perform the same above steps on the next character until all the character of block are complete, then take the next block and process it in the same manner until all the blocks of plain text are process .
15. **End**

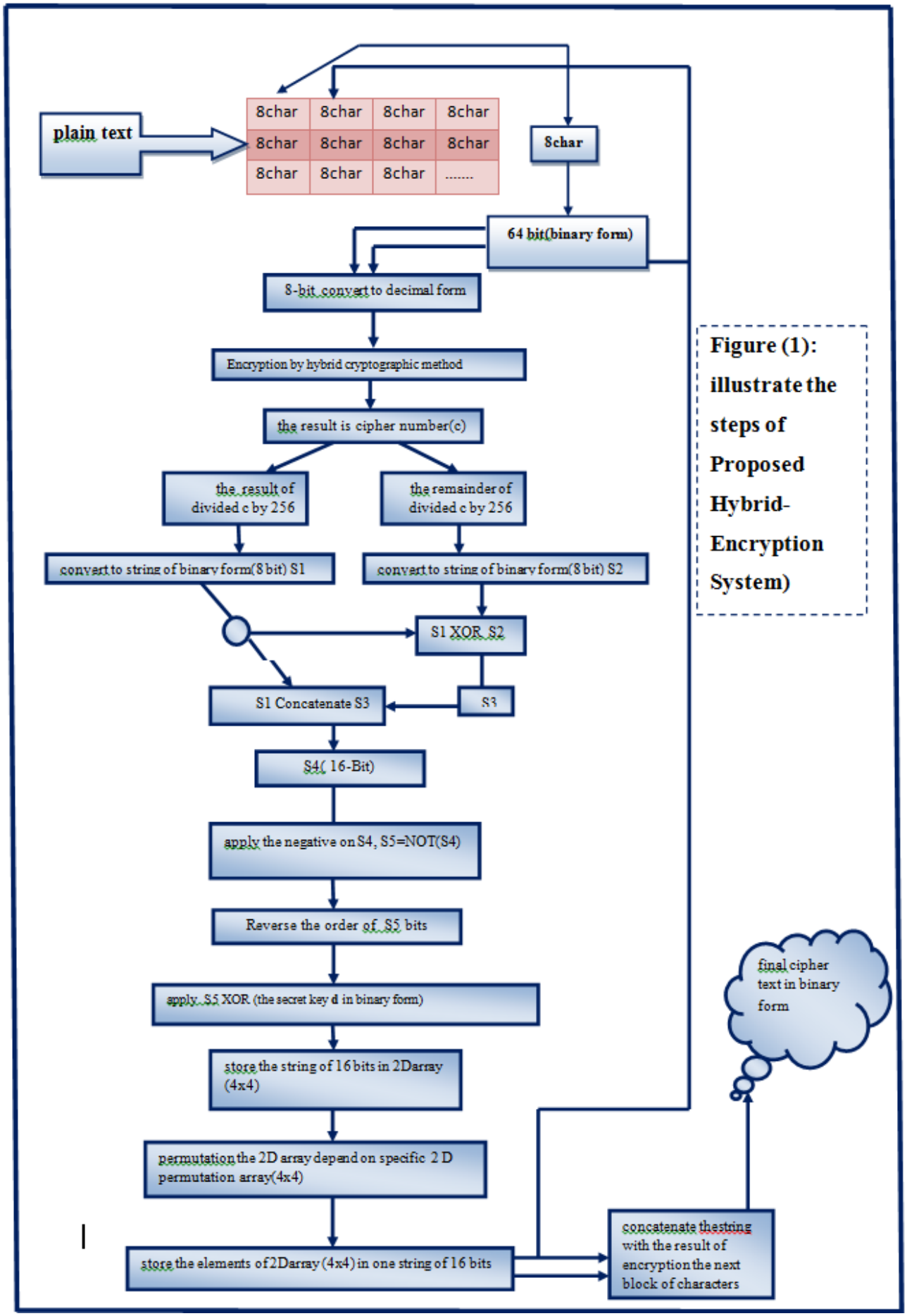


Figure (1): illustrate the steps of Proposed Hybrid-Encryption System)

1) Algorithm(A):Proposed Hybrid Public Key Method (Paillier and RSA)Initialization

In **The proposed hybrid public key method** the first step is to generatea keys, The keys are generated as follows:

1. **Begin**
2. Select two large prime numbers, p and q about the same size.
3. Compute the following :
   1) the modulus n the product of two primes **n =(p*q)**
   2) **λ = LCM (p - 1, q - 1)** (λ is Carmichael's function).
   3) Compute **φ(n) = (p-1)(q-1).**
   4) Select random integer **g** where **g** ∈ $Z^*_{n^2}$where g's order being a non zero multiple of n This can done efficiently by checking **gcd (L (g mod n2),n)**=1
   5) Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: **μ=L (g∈mod n^2) $^{-1}$mod nL(u)=u-1\ n for u =1 mod n(Lagrange function)**
   6) Choose an integerβ**, 1 <**β**<φ(n),** such that **gcd(**β**, φ(n)) = 1**.
   7) Compute the secret exponent **d, 1 < d <φ(n),** such that **β.d ≡ 1 (mod φ(n)).**

4.Publish the public key, (n, g,), and keep the private key(**μ,d,** λ) secret .

5. End.

Algorithm(B):The Proposed Hybrid Method (Paillier and RSA) Encryption

- **Input:** Plain text, Keys.
- **Output:** The cipher text(decimal numbers).
- **Begin**
- The cipher text **C< n^2**.
- Calculate γ, Where γ=**m** $^{\beta}$ mod n.
- Compute **the**cipher text **=g**$^{\gamma}$ · **β**^{n} **mod n^2.**
- Where **C**=**g**$^{m^{\beta} \bmod n}$ ·**β**$^{(p.q)}$ **mod** n^2
- **End**

Algorithm(C):The Proposed Hybrid Method (Paillier And RSA) Decryption

Input: The received encrypted cipher text , private keys**.**

Output: The original plaintext.

- **begin**
- Let C be the cipher text to decrypt, where **C**∈ $Z^*_{n^2}$

- Compute the plaintext message as: M = $\frac{L(C^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$

  or by substitution the value of **($\mu = L(g \in \bmod n^2)^{-1} \bmod n$)** the plaintext message can compute as follow :$M = L(C^{\lambda} \bmod n^2).\mu \bmod n$

- **End**

2)2D Permutation Array (PA)

The specific 2D array (4x4)used to permutation the elements of the array

(3,3)	**(2 , 2)**	**(0 , 0)**	**(1 ,1)**
(1 ,2)	**(0 , 1)**	**(3 , 1)**	**(2 , 1)**
(2 , 4)	**(3, 2)**	**(1, 3)**	**(0 , 2)**
(0 , 3)	**(1 , 0)**	**(3, 0)**	**(2 , 0)**

Figure(2): 2D array permutation (4x4)

(0 , 0)	**(0 ,1)**	**(0 , 2)**	**(0 ,3)**
(1 , 0)	**(1 ,1)**	**(1 ,2)**	**(1, 3)**
(2,0)	**(2 , 1)**	**(2 ,2)**	**(2 ,3)**
(3 ,0)	**(3 , 1)**	**(3,2)**	**(3 ,3)**

Figure(3): 2D array permutation inverse (4x4)

5.2 .The proposed algorithm fordecryption process (Figure (4): illustrate the steps of Proposed Hybrid-Decryption System)

Input: String of bit represent cipher text in binary form , keys.

Output: M as string of characters

1. **Begin**
2. Divided the input string into blocks each one with 128 bits and process on block (bi)each time .
3. Divided the block (bi) into 8- sub block (bij) each block is 16 bits(j=1-8)
   (i=length of cipher string of bits /128)
4. Store the string of bits of block (bij) into 2Darray (4x4), and Perform inverse permutation (inverse permutation of array can perform by retrieve the original order to the elements of array as shown in **Figure(3)**).

5. Convert the 2Dpermutedarray elements into one string with length 16 bits (S5).
6. Perform ((S5 XORS6) (where S6=the secret key **d** in binary form)).
7. Reverse the order of bits of new S5.
8. Perform NOT (S5) that give string (S4)
9. Divided the s4 into 2 string (1-8 bits store in S1)and (9-16 bits store in S3)
10. perform (S1 XOR X3) that give S2
11. Convert S1 to decimal number D1, convert S2 to decimal number D2
12. Using D1,D2 to retrieve the cipher number (C)
13. Decryption the (**C**) by using**The Proposed hybrid public key method(Algorithm(A),(Algorithm(C)).**
14. Convert the result number to character
15. Perform the above steps on the next 16-bits (bij) until complete all sub block, then process he next block of cipher text

End. (Figure (4): illustrate the steps of Proposed Hybrid-Decryption System)

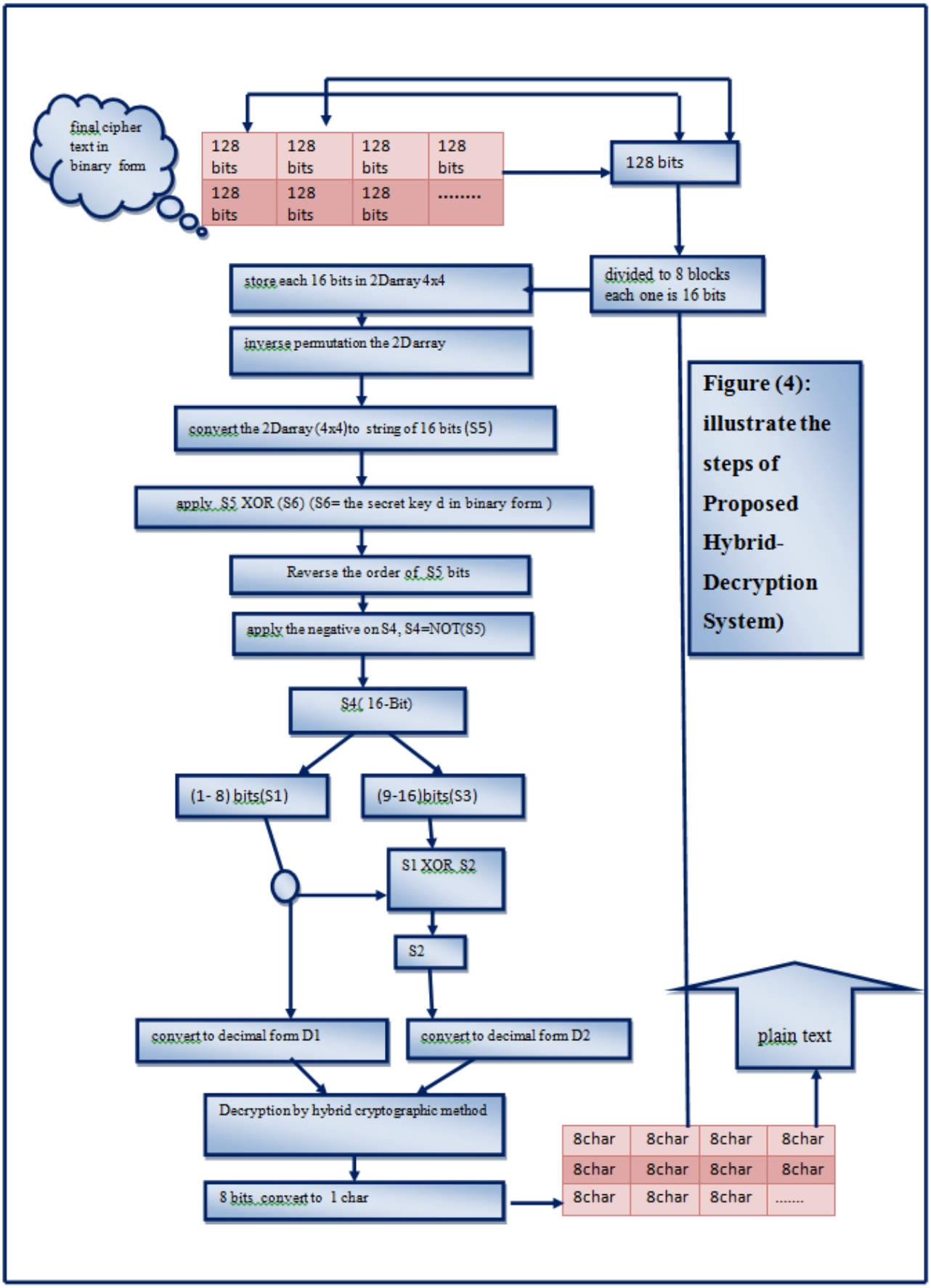


Figure (4): illustrate the steps of Proposed Hybrid-Decryption System)

6. The Results Of The Proposed Encryption Algorithm.

The proposed methods was implemented through Visual Basic.NET 2008 programming language on laptop (Intel(R)core(TM)i7-4500U CPU@1.80 2.40 GH_Z and RAM 6.00 GB)by Using a message with different size , To ensure the efficiency of the proposed methods, a various size of plaintext is assumed such as (7KB, 9KB, 10 KB, 11KB and 15MB). The following results represent the execution time (in second) of the both encryption and decryption operations for the proposed methods as show in table (1).

Table (1)Total Time Of The Proposed Method (In Sec.)

Message size	Operation	Proposed Method
7K	Encryption Decryption	Less than 1sec. Less than 1sec.
9K	Encryption Decryption	1 sec. 1 sec.
10K	Encryption Decryption	1sec. 1sec.
11K	Encryption Decryption	2 sec. 2sec.
15K	Encryption Decryption	3 sec. 3 sec.

- The minimum size of numbers that used in execution of program is n=8 bits , n^2= 16 bits , p =8bits, β=8bits

7. Conclusions

Several conclusions are reached through the working the system steps. The following items represent the important conclusions which are drawn from the proposed system:

1. The experimental results show that the complexity and the execution time of the public-key cryptosystems are trade-off problem, this means when the complexity degree increases the run time increases also but in little amount.

2. the security of the proposed hybrid system it based on (1- composite degree residues,2- factoring large numbers, 3- randomness)that will increase the complexity of proposed system analyzing and make it strong more than the original method and that proves by :

(A) the security Paillier cryptosystem algorithm based on the use of composite degree residues. and it provably secure under adequate intractability assumptions (it provide semantic security against chosen-plaintext attacks).

(B) The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers and the RSA problem

As it know, there are several algorithms used to solve the factorization problem (hard)such as NFS (Number Field Sieve), but when the used number be complex as much as it possible these type of algorithms become inefficient to work, therefore the proposed methods depend on this idea.)

(C) The using of (logic operations (NOT,XOR)will increase some of randomness on the cipher message because the statues of bits will change ,also the permutation operation change the locations of bits in cipher string)

References

1. Stallings W. (1999) Cryptography and Network Security, Principle and Practice ", Addison Wesley.
2. **Gary c.** Kessler. (2007) An Overview of Cryptography URL:http://www.garykessder.net/library/crypto.html.
3. RSA cryptosystem - Wikipedia, the free encyclopedia **URL:http://www.**en.wikipedia.org/wiki/**RSA_cryptosystem**, 2015.
4. **Van Oorschot** M. P., Vanstone S. (1996) Handbook of applied cryptography, CRC Press, 1996.
5. **Adler M.,** Gailly J. (2004) **An Introduction to Cryptography**", PGP Corporation.
6. Paillier. (2015) cryptosystem - Wikipedia, the free encyclopedia **URL:http://www.**en.wikipedia.org/wiki/**Paillier_cryptosystem**.
7. Kert Richardson. (2006) Progress on Probabilistic Encryption Schemes. M.Sc thesis ,the Faculty of the Computer Science Department of the Rochester Institute of Technology.
8. Song.Y. Yan. (2002) Number theory for computing, Springer-Verlag, 2002.
9. Dorothy Elizabeth Rob, ling Denning,"Cryptography and data Security", Purdue University Vav Addison-Wesley Publishing Company Reading, 1982.16.