استخدام الشبكات العصبية في التشفير

شهلة حازم احمد خروفة

قسم العلوم الأساسية ، كلية طب الأسنان ، جامعة الموصل ،العراق

(تاريخ الاستلام: ١٧ / ٦ / ٢٠٠٩ ، تاريخ القبول: ٢٧ / ٤ / ٢٠١٠)

الملخص

إن الهدف الأساسي للتشفير هو الحفاظ على النص الصريح (أو المفتاح، أو كلاهما) بصورة سرية بعيداً عن الأعداء على افتراض أنهم يملكون كامل القدرة للوصول إلى الاتصالات بين المرسل والمستقبل. والتشفير عموما هو نقل بيانات من طرف إلى طرف أخر وذلك مع حفظ البيانات من التغير والتعديل والإطلاع. وهناك عدة طرق للتشفير تستخدم لتحويل الرسالة الأصلية إلى رسالة مشفرة ، أما الشبكات العصبية الاصطناعية فهي نظام معالجة المعلومات له مميزات أداء معينة بأسلوب يُحاكي الشبكات العصبية الحيوية . وبصيغة أخرى نجد أن الشبكات العصبية الاصطناعية إنما هي محاكاة للطريقة التي يؤدي بها العقل البشري مهمة معينة، وهو عبارة عن معالج ضخم موزع على التوازي، ومكون من وحدات معالجة بسيطة، بحيث يقوم بتخزين المعرفة العملية ليجعلها متاحة للمستخدم وذلك عن طريق ضبط الأوزان.

وفي هذا البحث تم استخدام الشبكات العصبية في التشفير إذ تم استخدام شبكة الانتشار الخلفي التراجعي لتنفيذ العمل نظراً لما تتميز به هذه الشبكة من ميزات عديدة من سهولة في التعامل مع المسائل باسلوب واضح وبسيط وامكانية الشبكة من حل المسائل المعقدة واستخدامها في تميز الأنماط وتضمن العمل مرحلتين: المرحلة الأولى تم اقتراح خوارزمية لعملية التشفير إذ يتم إدخال النص الصريح ويتم الحصول على النص المشفر باستخدام الشبكة أما المرحلة الثانية فقد تم اقتراح خوارزمية لعملية كسر الشفرة إذ يتم إدخال النص المشفر ويتم الحصول على النص الصريح باستخدام الشبكة.

تم عمل برنامج بلغة (Matlab Version 6.5) لتنفيذ العمل.

1- التشفير:

التشفير عبارة عن طريقة يتم فيها إخفاء المعلومات عن طريق مفتاح سري وخوارزمية، الذي يعلم المفتاح ويعلم خوارزمية التشفير يمكنه فك الشفرة (أي استعادة المعلومات الأصلية). والتشفير عالم ضخم بما يحتويه من علم ومعلومات وأفكار وطرق وسُبل في جعل المعلومات أياً كانت رسائل إلكترونية أو ملفات أو عبارات أو رموز مشفره مغلفة بغلاف لا يستطيع أحد فهمه. وبالتأكيد هناك طرق للتشفير قديمة وهنالك طرق حديثة[1].

والتشفير هي طريقة لإرسال المعلومات بحيث يستطيع الأشخاص الذين لديهم مفتاح خاص فقط الاطلاع عليها وفهمها بينما لا يستطيع أي شخص آخر لا يملك المفتاح معرفتها ، وقد تكون هذه المعلومات رسائل مكتوبة أو محادثات هاتفية أو صور أو بيانات تنقل عبر وسائل الاتصالات الحديثة أو تحفظ وتعالج بوساطة الحواسيب. ومع التقدم السريع والمتنامي لوسائل نقل المعلومات (الاتصالات) ووسائل تخزينها ومعالجتها (الحواسيب)، فإن أهمية الرسائل المكتوبة أو البريد بدأت تتضاءل من ناحية، ومن ناحية أخرى، ازدادت الحاجة إلى الحفاظ على أمن المعلومات وسريتها. والتشفير هو أهم طرق حماية المعلومات وأكثرها كفاءة خصوصاً إذا كانت المعلومات ستنقل على شبكات اتصال سلكية أو لاسلكية يسهل التنصت عليها، أو كانت المعلومات تتبادل في شبكات الحواسيب الحديثة الواسعة الانتشار التي يمكن اختراقها [2] [1].

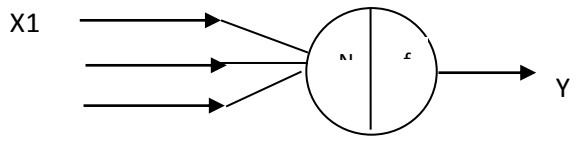
ويعالج هذا العلم مسألتين: تتناول الأولى طرق إخفاء المعلومات المرسَلة من جهة لأخرى وهو ما يسمى بالتشفير ، وتختص الثانية بطرق استخراج المعلومات من قِبَل الملتقط للرسائل المشفرة، وذلك بدون معرفة المفتاح المتفق عليه بين المتراسلين، وهو ما يسمى بكسر الشفرة. فالمشفر أو واضع التشفير يهدف إلى ضمان سرية الرسالة أو إلى ضمان أصالتها وحمايتها من التحريف أو الادعاء. أما محلل الشفرة أو (العدو)، فيسعى إلى الهدف المضاد المتمثل في كسر الشفرة ومعرفة محتوى الرسالة السرية أو تحريف محتوى الرسالة، أو تزويرها بشكل يؤدي إلى قبولها على أنها رسالة صحيحة أو أصلية وهي غير ذلك [3]. فهدف التشفير هو ضمان سرية الرسالة أو حماية محتوياتها أو مصدرها من التحريف أو التزوير، بينما يهدف تحليل التشفير إلى عكس ذلك تماماً[1] .

2- الشبكات العصبية:

الشبكات العصبية الاصطناعية هي أحد الاتجاهات الحديثة في تطبيقات الحواسيب الالكترونية جاءت بديلاً عن الأساليب التقليدية في البرمجة التي واجهت معاضل كبيرة وأساسية في بعض التطبيقات الحديثة، وانتهجت محاكاة معمارية وأسلوب عمل الأنظمة الطبيعية كمحاولة جادة للوصول إلى إنتاج أجهزة وبرامج ذكية[5][4].

والشبكة العصبية مصممة كنظام لمعالجة المعلومات متصلة بينياً وهذه العناصر المعالجة قادرة على التعلم عن طريق استلام المدخلات الأكثر وزناً ومع التعديلات والتوقيت والتكرار يمكن لهذه العناصر إنتاج مخرجات صالحة[6].

تعرف الشبكة العصبية الاصطناعية على أنها نظام حسابي مكون من عدد من وحدات المعالجة المترابطة مع بعضه وتتصف بطبيعتها الديناميكية والمتوازية في معالجة البيانات الداخلة إليها. وتعتبر الخلية العصبية الاصطناعية هي وحدة بناء الشبكة العصبية الاصطناعية وتتكون الخلية العصبية الاصطناعية من وحدة حسابية متعددة المداخل واشارة خارجة واحدة ولكل اشارة داخلة هناك وزن يعمل على تعديل الاشارة الداخلة ويعمل على تحفيز الخلية لإنتاج اشارة رد فعل عندما تكون قيمته موجبة أو إخمادها وتقليل الاشارة الخارجة عندما تكون قيمته سالبة [8][7]. لاحظ الشكل رقم (1)



الشكل رقم (1) الخلية العصبية الاصطناعية

يمكن تمييز ثلاثة أنواع من التعليم في الشبكات العصبية الاصطناعية وهي:

١ – التعليم الموجه

يتم التعليم بإدخال زوج مكون من (الإدخال والخراج المطلوب) وتعدل الأوزان بالاعتماد على الفرق بين الإخراج المطلوب والإخراج الحقيقي، ويستمر التعليم إلى أن يصبح الفرق بين القيمتين مقارباً للصفر، واشهر شبكات هذا النوع من التعليم شبكة الانتشار التراجعي[9].

٢ – التعليم غير الموجه

لا نحتاج هنا لوجود الإخراج المطلوب ونكتفي بتسليط الإدخال حيث تحدث عملية تنظيم ذاتي بالاعتماد على خوارزمية تعليم معينة بدون الإخراج المطلوب، واشهر شبكتين من هذا النوع هما شبكة كوهين (Kohonen) وشبكة كروسبيرك (Grossberg) [10].

٣ – التعليم القسري

هي طريقة تعليم تشبه التعليم الموجه، ولكن لا يوجد إخراج مطلوب محدد بل بوجد مؤشر يحدد صحة أو خطا الإخراج حيث تعدل الأوزان اعتماداً على ذلك وتزداد الأوزان في حالة كون إجابة المؤشر صائبة وبعكسه ستقلل الأوزان[11].

2-1 شبكة الانتشار الخلفي التراجعي Back Propagation Neural Net work:

2-1-1 المقدمة

كان العالم ويرباس (Werbos) أول من تطرق لفكرة شبكة الانتشار التراجعي ثم روملهارت (Roomelhart) وهينتن (Hinton) ووليامس (Williams) حيث تم نشر هذه الفكرة[13][12]. وتستخدم هذه الشبكة في الكثير من التطبيقات وذلك لأنها تمتلك عمومية في التعامل مع كافة أنواع المسائل وأنها واسعة الانتشار وسهلة التعامل مع الكثير من المسائل باسلوب واضح وبسيط ويضاف إلى ذلك استخدامها في تمييز الأنماط وكذلك تستعمل مع الكثير من المسائل المعقدة التي لا يمكن استخدام الشبكات الأخرى معها حيث أنها تستخدم في التشخيصات المرضية [14] [15] [16].

2-1-2 مميزات الشبكة:

١–تعتبر الشبكة ذات تعليم موجه(Supervised Learning) أي أنها تحتوي على الإدخال والإخراج المطلوب [9].

٢–الوزن لها يكون عبارة عن مصفوفة ذات قيم صغيرة عشوائية (Small real number) [17].

٣–الربط فيها يتكون من مرحلتين: المرحلة الأولى مرحلة Forward أي انسياب المدخلات باتجاه المخرجات، والمرحلة الثانية هي مرحلة Back propagate أي انسياب أو رجوع الخطأ من الإخراج باتجاه الإدخال[19][18].

٤–البيانات الداخلة تكون أما ثنائية أو مستمرة[21][20].

٥–تتكون الشبكة من عدة طبقات (Multi layers) [24][23][22].

٦–تكون دالة التحفيز لها هي السغمويد (Sigmoid function) وهذه الدالة تمتاز بعد خصائص حيث تكون غير خطية وإدخالاتها تكون مستمرة والمشتقة لها بسيطة[25].

٧–يغير الوزن لتقليل نسبة الخطأ التي ينتج من الشبكة[26].

٨–شرط توقف الشبكة هو الحصول على الإخراج المطلوب أي[17]:

- Desired out put = Actual out put
- الاقتراب من الحل الصحيح بأقل خطأ ممكن
- يتم تحديد عدد الدورات مسبقاً

2-1-3 أطوار الشبكة:

لشبكة الانتشار الخلفي التراجعي طورين هما[29][28][27]:

١– طور التعلم: أي تدريب الشبكة على النمط المعطى وفيه تغذية أمامية وخلفية.

- التغذية الأمامية Feed Forward: انسياب البيانات من خلايا الإدخال باتجاه خلايا الإخراج.
- انسياب الخطأ خلفاً Back Propagation: رجوع الخطأ (Error) من طبقة الإخراج باتجاه الإدخال للحصول على الأوزان المثالية.

٢–طور التذكر: أي اختبار الشبكة هل دربت على النمط المعطى أم لا أي هل حصلنا على الوزن المثالي أم لا وفيه فقط تغذية أمامية (Feed Forward).

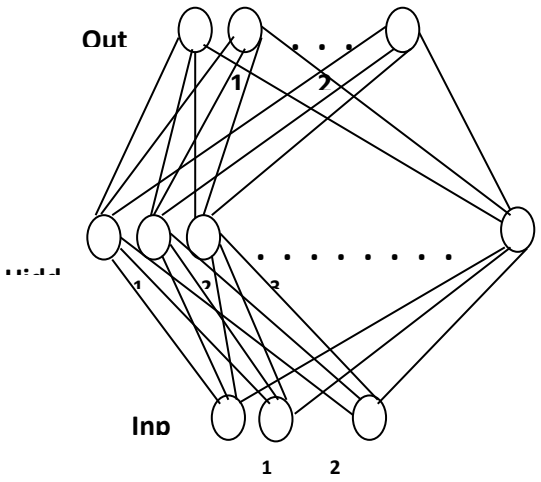
2-1-4 معمارية شبكة الانتشار الخلفي التراجعي المستخدمة في التشفير:

تتكون شبكة الانتشار الخلفي التراجعي التي تم استخدامها في التشفير من ثلاث طبقات كما مبين في الشكل رقم (2) وهي:

١– طبقة الإدخال (Input layer) تتضمن أربع عقد وتكون بعدد المفاتيح المستخدمة (k1, k2, k3, k4).

٢– الطبقة الخفية (Hidden layer) وتتضمن ستة عشر عقدة وهي تمثل عدد الحالات أي 2^N حيث أن N تمثل عدد المفاتيح.

٣– طبقة الإخراج (Output layer) وتتضمن سبعة عقد (وذلك لان اكبر رقم من مجموع أرقام المفاتيح يساوي 100 وهو يأخذ 7 bit عند تمثيلة بالنظام الثنائي).



الشكل رقم (2) معمارية الشبكة المستخدمة في التشفير

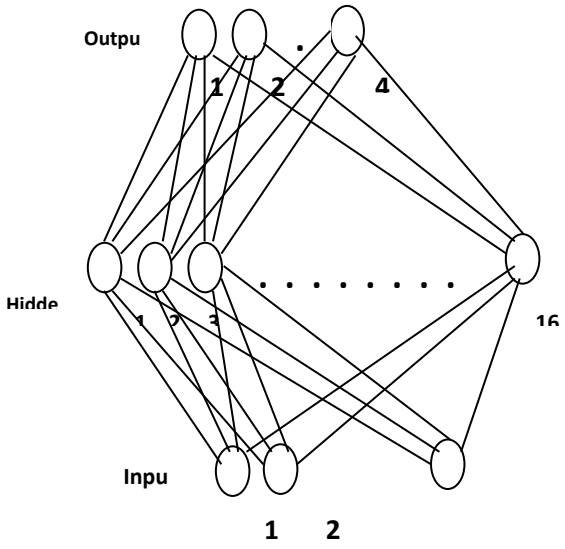
2-1-5 معمارية شبكة الانتشار الخلفي التراجعي المستخدمة في فك الشفرة:

تتكون شبكة الانتشار الخلفي التراجعي التي تم استخدامها في فك الشفرة من ثلاث طبقات كما مبين في الشكل رقم (3) وهي:

١– طبقة الإدخال (Input layer) وتتضمن سبعة عقد.

٢- الطبقة الخفية (Hidden layer) وتتضمن ستة عشر عقدة.

٣- طبقة الإخراج (Output layer) وتتضمن أربعة عقد.



الشكل رقم (3) معمارية الشبكة المستخدمة في فك الشفرة

6-1-2 النقاط الملاحظة عند تصميم الخوارزميتين المقترحتين:

تم اقتراح خوارزميتين الأولى للتشفير والأخرى لكسر الشفرة باستخدام شبكة الانتشار الخلفي التراجعي وعند التصميم تم ملاحظة النقاط التالية:

١- اختيار المفاتيح بشكل مناسب مع مراعاة الشروط التالية:

- اختيار قيم المفاتيح بشكل عشوائي على شرط ($k1 \neq k2 \neq k3 \neq k4 \neq 0$) وتم في هذا البحث اختيار القيم التالية للمفاتيح (k1=2, k2=14, k3=55, k4=29).
- مجموع أي قيم من المفاتيح (التي قيم الـbit فيها يساوي واحد) لا يساوي مجموع أي من قيم المجاميع الأخرى كما مبين في الجدول رقم (2) أي: ($100 \neq$ --------- $\neq 55 \neq 29 \neq 0$)

٢- التعامل مع رسالة الإدخال بشكل دقيق حيث تم مراعاة أن الرسالة ممكن أن تحتوي على الحروف الكبيرة والصغيرة الأرقام والرموز كما مبين في الجدول رقم (1).

٣- عند إجراء عملية التشفير يكون الإدخال (Input) إلى الشبكة متكون من (4 bit) أما الإخراج (Desire output) متكون من (7 bit) كما مبين في الجدول رقم (2).

٤- عند إجراء عملية فك الشفرة يكون الإدخال (Input) إلى الشبكة متكون من (7 bit) أما الإخراج (Desire output) متكون من (4 bit) كما مبين في الجدول رقم (3).

الجدول رقم (1) يوضح الأحرف والأرقام والرموز وتسلسلاتها التي ممكن أن تكون موجودة في أي نص مطلوب تشفيره

ت	الرمز	ت	الرمز	ت	الرمز	ت	الرمز	ت	الرمز	ت	الرمز
1		17	<	33	.	49	P	65	`	81	p
2	!	18	=	34	A	50	Q	66	a	82	q
3	"	19	>	35	B	51	R	67	b	83	r
4	#	20	؟	36	C	52	S	68	c	84	s
5	$	21	:	37	D	53	T	69	d	85	t
6	%	22	0	38	E	54	U	70	e	86	u
7	&	23	1	39	F	55	V	71	f	87	v
8	'	24	2	40	G	56	W	72	g	88	w
9	)	25	3	41	H	57	X	73	h	89	x
10	(	26	4	42	I	58	Y	74	i	90	y
11	*	27	5	43	J	59	Z	75	j	91	z
12	+	28	6	44	K	60	[	76	k	92	DEL
13	،	29	7	45	L	61	\	77	l	93	~
14	-	30	8	46	M	62	]	78	m	94	{
15	@	31	9	47	N	63	^	79	n	95	|
16	؟	32	/	48	O	64	_	80	o	96	}

الجدول رقم (2) يوضح الإدخال والإخراج ومجموع قيم المفاتيح التي قيمة الـ(bit=1) لشبكة الانتشار الخلفي التراجعي المستخدمة في التشفير

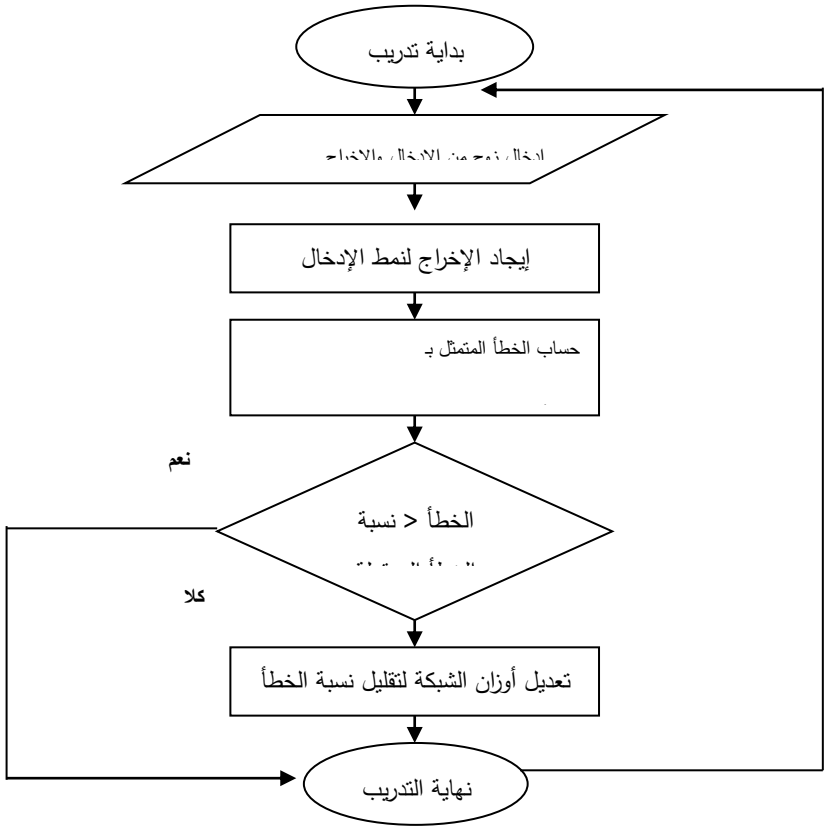
الإدخال (Input)					الإخراج (Output)						
المجموع	K1	K2	K3	K4	C1	C2	C3	C4	C5	C6	C7
0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	1	0	0	1	1	1	0	1
55	0	0	1	0	0	1	1	0	1	1	1
84	0	0	1	1	1	0	1	0	1	0	0
14	0	1	0	0	0	0	0	1	1	1	0
43	0	1	0	1	0	1	0	1	0	0	1
69	0	1	1	0	1	0	0	0	1	0	1
98	0	1	1	1	1	1	0	0	0	1	0
2	1	0	0	0	0	0	0	0	0	1	0
31	1	0	0	1	0	0	1	1	1	1	1
57	1	0	1	0	0	1	1	1	0	0	1
86	1	0	1	1	1	0	1	0	1	1	0
16	1	1	0	0	0	0	1	0	0	0	0
65	1	1	0	1	1	0	0	0	0	0	1
71	1	1	1	0	1	0	0	0	1	1	1
100	1	1	1	1	1	1	0	0	1	0	0

الجدول رقم (3) يوضح الإدخال والإخراج لشبكة الانتشار الخلفي التراجعي المستخدمة في فك التشفير

الإدخال (Input)							الإخراج (Output)			
C1	C2	C3	C4	C5	C6	C7	K1	K2	K3	K4
0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	1	0	0	0	1
0	1	1	0	1	1	1	0	0	1	0
1	0	1	0	1	0	0	0	0	1	1
0	0	0	1	1	1	0	0	1	0	0
0	1	0	1	0	0	1	0	1	0	1
1	0	0	0	1	0	1	0	1	1	0
1	1	0	0	0	1	0	0	1	1	1
0	0	0	0	0	1	0	1	0	0	0
0	0	1	1	1	1	1	1	0	0	1
0	1	1	1	0	0	1	1	0	1	0
1	0	1	0	1	1	0	1	0	1	1
0	0	1	0	0	0	0	1	1	0	0
1	0	0	0	0	0	1	1	1	0	1
1	0	0	0	1	1	1	1	1	1	0
1	1	0	0	1	0	0	1	1	1	1

7-1-2 مخطط تدريب الشبكة:

تم استخدام المخطط الموضح في الشكل رقم (4) في تدريب الشبكة وهو:



الشكل رقم (4) يوضح المخطط الانسيابي المستخدم في تدريب الشبكة

3 خوارزمية التشفير المقترحة:

تم اقتراح الخوارزمية التالية لعملية التشفير باستخدام شبكة الانتشار الخلفي التراجعي وهي:

١- إدخال النص الصريح

٢- إيجاد حجم النص الصريح ووضعه في المتغير N

٣- F=1

٤- اخذ حرف من النص وإيجاد تسلسله حسب الجدول رقم (1) واخذ التسلسل وجمعه مع 100

٥- تحويل الناتج إلى النظام الثنائي

٦- F=F+1

٧- إذا كان (F<=N) الرجوع إلى الخطوة رقم ٤

٨- الحصول على مصفوفة ثنائية عدد الصفوف فيها بعدد أحرف النص الصريح وعدد الأعمدة فيها8

٩- ندرب الشبكة حسب الشكل رقم (3) على الجدول رقم (2)

١٠- تحويل المصفوفة الثنائية إلى مصفوفة أحادية اسمها X1 وإيجاد حجمها ووضعه في المتغير N1

١١- F=1

١٢- اخذ (4 bit) من المصفوفة X1 ونختبر الشبكة ونحصل على الإخراج ويتكون من (7 bit)

١٣- F=F+4

١٤- إذا كان (F<=N1) الرجوع إلى الخطوة رقم ١٢

١٥- الحصول على النص المشفر والمتمثل بمصفوفة أحادية

والمخطط الانسيابي لعملية التشفير باستخدام شبكة الانتشار الخلفي التراجعي موضح في الشكل رقم (5)

4- خوارزمية فك الشفرة:

تم اقتراح الخوارزمية التالية لعملية فك الشفرة باستخدام شبكة الانتشار الخلفي التراجعي وهي:

١- إدخال النص المشفر

٢- إيجاد حجم النص المشفر ووضعه في المتغير N

٣- ندرب الشبكة حسب الشكل رقم (4) على الجدول رقم (3)

٤- F=1

٥- اخذ (7 bit) من النص المشفر ونختبر الشبكة ونحصل على الإخراج ويتكون من (4 bit)

٦- F=F+7

٧- إذا كان (F<=N) يتم الرجوع إلى الخطوة رقم ٥

٨- وضع الناتج في مصفوفة أحادية اسمها Y1 وإيجاد حجمها ووضعه في المتغير N1

٩- F=1

١٠- اخذ (8 bit) من Y1 ونحولها من النظام الثنائي إلى النظام العشري

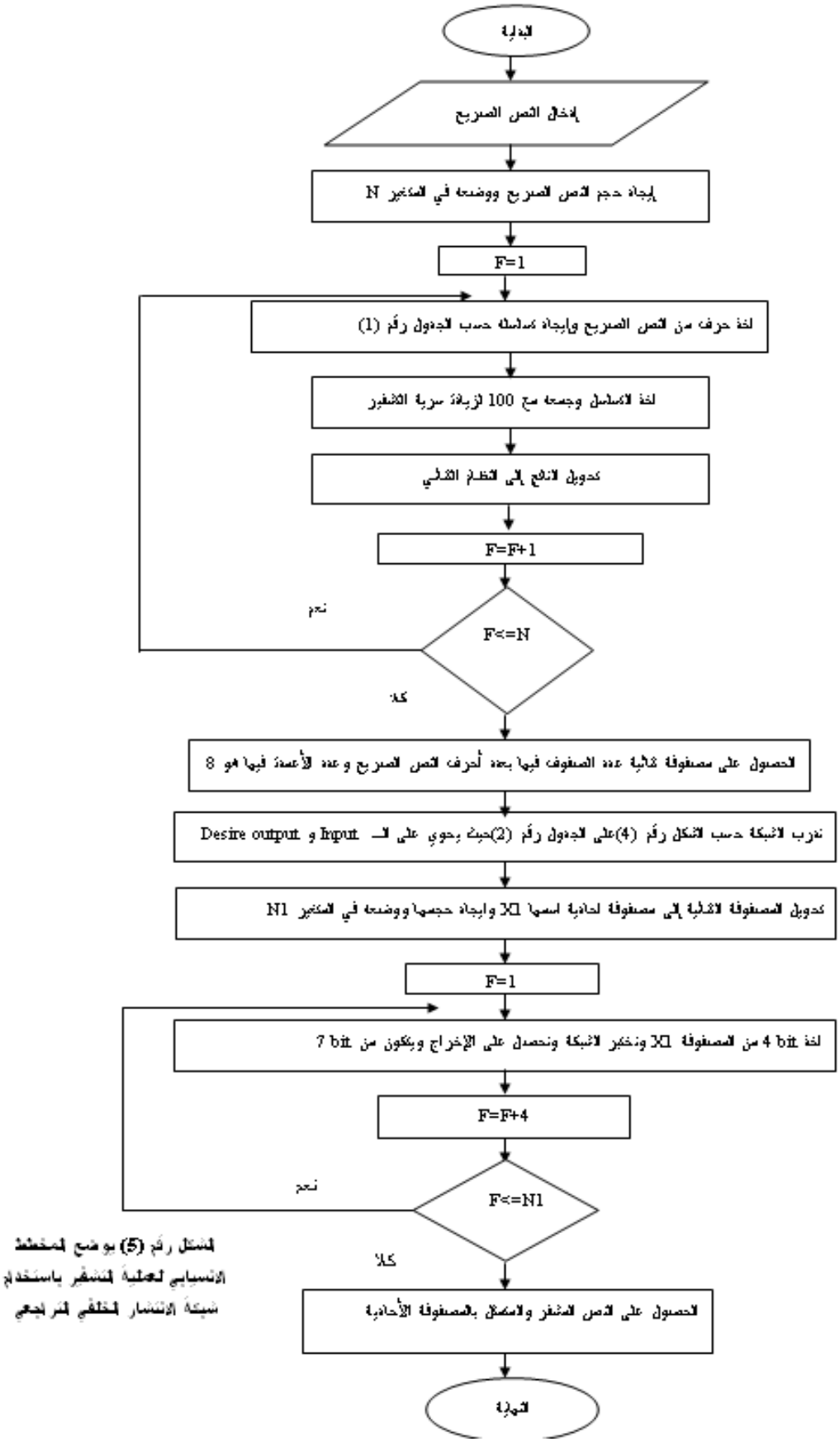
١١- طرح 100 من الناتج

١٢- بالاستعانة بالجدول رقم (1) يتم إيجاد (الحرف، الرقم، الرمز) المستخدم ويتم وضعه في مصفوفة أحادية وهذا يمثل النص الصريح

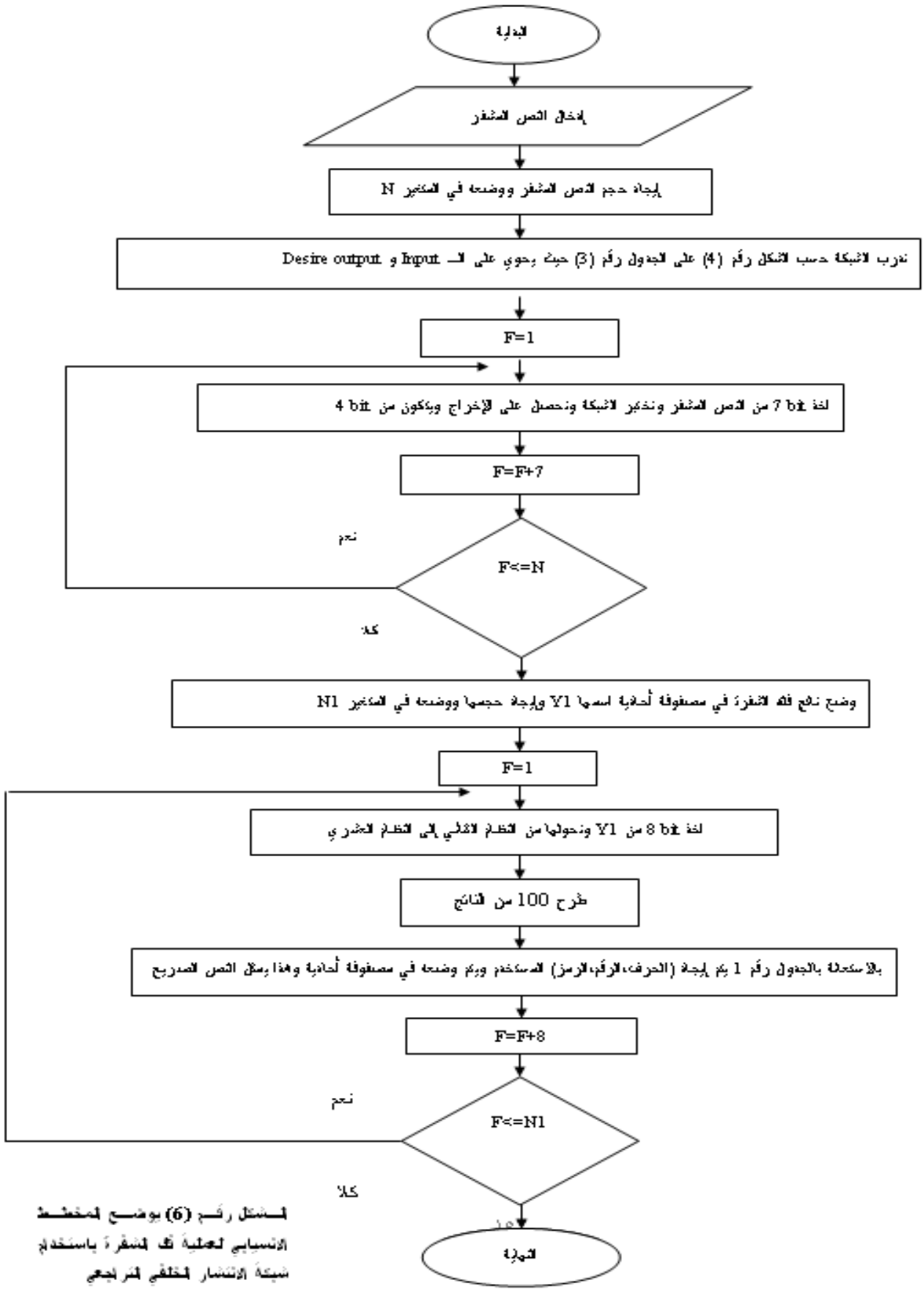
١٣- F=F+8

١٤- إذا كان (F<=N1) يتم الرجوع إلى الخطوة رقم ١٠

والمخطط الانسيابي لعملية فك الشفرة باستخدام الشبكة موضح في الشكل رقم (6).



الشكل رقم (5) يوضح المخطط الانسيابي لعملية التشفير باستخدام شبكة الانتشار الخلفي المتراجعي



الشكل رقم (6) يوضح المخطط الانسيابي لعملية فك الشفرة باستخدام شبكة الانتشار الخلفي الراجعي

5 - الاستنتاجات:

التشفير في أبسط تعريف له هو تحويل نص واضح (مكتوب أو منطوق) إلى نص غير مفهوم باستخدام طريقة محددة تعتمد على مفتاح سري خاص بالمتراسلين، بحيث يستطيع من يملك هذا المفتاح (ويعرف الطريقة) أن يعيد النص المشفر إلى أصله الواضح (يستخرج الشفرة)، بينما لا يستطيع أي شخص أخر لا يملك هذا المفتاح السري أن يتوصل إلى النص الواضح حتى وإن كان يعرف تفاصيل طريقة التشفير. أما تعريف كسر الشفرة فهو عملية استخدام النص المشفر للتوصل إلى النص الواضح، وذلك من محلل الشفرة.

وما الشبكات العصبية إلاّ محاولة لفهم أعمق وأوضح لعمل وسلوك الشبكة العصبية الحيوية، ومن هنا كان لابد من إقامة علاقة وثيقة بين الشبكات العصبية الحيوية والشبكات العصبية الاصطناعية من حيث البنية والتفصيل ليُصار إلى دفع تقنيات الذكاء الاصطناعي إلى الأمام . وما كان ذلك إلاّ كما ذكرت سابقاً (بمحاكاة الشبكة العصبية الحيوية بالشبكة العصبية الاصطناعية).

وفي هذا البحث تم استخدام الشبكات العصبية في التشفير إذ تم استخدام شبكة الانتشار الخلفي التراجعي لتنفيذ العمل نظراً لما تتميز به هذه الشبكة من مميزات عديدة حيث تم اقتراح خوارزميتين: الأولى استخدمت للتشفير حيث أن النص الصريح ممكن أن يحتوي على أي (حرف، رقم، رمز) وممكن أن يكون بأي حجم، كما تم اختيار المفاتيح بصورة عشوائية مع مراعاة بعض الشروط الواجب توفرها. أما االخوارزمية الثانية استخدمت لفك الشفرة حيث يتم إدخال النص المشفر وبالاعتماد على الشبكة يتم فك الشفرة والحصول على النص الصريح.

وقد أظهرت الخوارزميتين اداء عالي في التشفير وفي فك الشفرة عند تنفيذها على عدد من النصوص حيث كانت نتائج الاختبار جيدة وتم الحصول على اداء أفضل من استخدام طرق التشفير الاعتيادية.

6 -المصادر:

1. Shihab, Khalil, A back propagation neural network for computer network security, Journal of computer science ISSN, (2006): P 710-715.
2. Elsevier, Network and information security: a computational intelligence approach, Journal of network and computer applications, (2007): P 1-3.
3. Yang, Jiyun Xiaofeng Liao, Cryptanalysis of cryptographic scheme based on delayed chaotic neural networks, ELSEVIER, (2007): P 1-5.
4. Antonie, Maria Luiza Osmar R. and Alexandru Loman, Application of data mining techniques for medical image classification, ACM SIGKDD Conference, , (2001): P 94-101.
5. Babovic, Vladan M. , Seabed recognition using neural networks, Technical Report, Danish Hydraulic Institute, (1999): P 1-74.
6. Chang, Ping and Jeng Shong Shih, The application of back propagation neural network of multi-channel piezoelectric quartz crystal sensor for mixed organic vapours, Tamkang Journal of science and engineering, Vol. 5, No. 4, (2002): P 209-217.
7. Mundhenk, T. Nathan and Michael A. Arbib, Back-propagation neural network homework, CSCI, (2006): P 1-7.
8. Vesely, A., Neural networks in data mining, AGRIC. ECON.-CZECH, (2003): P 427-431.
9. Tsaregorodtsev, Victor G., Parallel implementation of back-propagation neural network software on smp computers, LNCS, (2005):P 186-192.
10. Jain, Anil K., Statistical pattern recognition: a review, IEEE, Vol. 22, No. 1, (2000): P 1-34.
11. Park, Hoasung, Fuzzy relation- based fuzz neural- networks using a hybrid identification algorithm, International Journal of control, Vol. 1, No. 3, (2003): P 1-12.
12. Kamruzzaman, Joarder Rezaul K. Ruhu, Artificial neural networks in finance and manufacturing, IDEA, , (2003):P 1-31.
13. Otair, Mohammed A. Walid A., Speeding up back propagation neural networks:, Informing science and IT education joint conference, (2005):P 1-7.
14. Ismail, Saliza, Recurrent neural network with back propagation through time algorithm for Arabic recognition, Proceedings 18th European Simulation Multi conference. (2004)
15. Betker, A. L. Szturm and Z. Moussavi, Application of feed forward back propagation neural network to center of mass estimation for use in a clinical environment, IEEE, (2003): P 2714-2717.
16. Durai, S. Anna and E. Anna Saro, Image compression with back propagation neural network using cumulative distribution function, ISSN, (2006): P 1-5.
17. Chang, Ray-I, Liang-Bia, Intrusion detection by back propagation neural networks with sample-query and attribute-query, International Journal of computational Intelligence Research ISSN., Vol. 3, No. 1, (2007):P 6-10.
18. Henning, Kai Thorsten dc, Multi sensor system for fast analysis in environmental monitoring with an application in waste water treatment, EARsel- SIG, No. 1, (2000):P 61-67.
19. Khan Asif Ullah T. K. Bandopadhyaya, Genetic algorithm based back propagation neural network performs better than back propagation neural network in stock rates prediction, IJCSNS, International Journal of computer science and network security, Vol. 8, No. 7, (2008): P 1-5.
20. Jantzen, Jan, Introduction to perceptron networks, DENMARK Tech report No., (1998):P 1-32.
21. Kusumaputre, Benyamin and Teguh P. Arsyad, Recognizing order mixtures using optimized fuzzy neural network through genetic algorithm, Journal of advanced computational Intelligence and Intelligent Informatics, Vol. 9, No. 3, (2005): P 290-291.
22. Valdes, Julia J., Behavior of similarity- based neuro- fuzzy networks and evolutionary algorithms in time series model mining, NRC-CNRC, (2002): P 1-6.

23. Nikravesh, Masoud F. Aminzadeh, Past, present and future intelligent reservoir characterization trends, Journal of petroleum science and engineering 31. , (2001): P 67-79.
24. Kasabov, Nikola Senior Member, Evolving fuzzy neural networks for supervised/ unsupervised, IEEE, Vol. 3, No. 6, (2001):P 1-67.
25. Moghadas, R. Kamyab and S. Gholizadeh, A new wavelet back propagation neural networks for structural dynamic analysis, Engineering letters, (2008): P 1-6.
26. Sajda, Paul, Learning contextual relationships in mammograms using a hierarchical pyramid neural network, IEEE, Vol. 21, No. 3. (2002).
27. Mitrassushmita,Senior Member, Data mining in soft computing framework a survey, IEEE, Vol. 13, No. 1. (2002).
28. Sharhui, Liu Yao Hongeun, Neural network based steganalysis in still image, IEEE, (2003): P 1-4.
29. Lakshmi, Seetha Shooyu Zhou, Selectivity estimation in extensible data bases - a neural network approach, 24th ULDB conference new york, (1998): P 1-5.

Using the Neural Networks in Encryption

S. H. Karruffa
Basic Sciences, College Of Dentistry, Mosul University, Iraq
(Received , Accepted)

Abstract

The main purpose of encryption is keeping the plain text (or the key or both) secretly far from the enemies on the assumption of being have the whole ability to reach the communications between the sender and the receiver. Encryption generally is data transportation from one side to another by keeping the data not to be change or amended or watching, There are many ways for encryption that are used for converting the original message to a cipher one. While the artificial neural networks are data processing system that has performance characteristics in a way that resembles the vital neural networks. In another form, we found that artificial neural networks is either a resemblance for the method that the human mind performs a certain mission, which is a huge processor that is distributed in parallel way and consisted of simple processing units where it stores the practical knowledge to make it available for user by means of weights seizing.

In this research, the neural network was used in encryption The back propagation neural network was used for performing the action, it has many characteristics can be easily treated with problems in a simple and clear way and the possibility of the network to solve the complex problems and using it in pattern recognition. is work includes two stage: The first stages, an algorithm was suggested for encryption process where plain text can be entered and getting the cipher text by using the neural network. While the second stage , an algorithm was suggested for the process of decryption were the cipher text can be entered and to produce the plain text by using network. The program was developed in Matlab language version 6.5 for performing the action.