Confirm Content Validity and Sender Authenticity for Text Messages by Using QR Code

Firas Mohammed Aswad **Yasir Ali Matni**

Inteasar Esmaeel Khudair **Ahmed Ehsan Mohammed**

University of Diyala, College of Basic Education

Altae13@yahoo.com ee22a12@gmail.com
Inteasar_yassin@yahoo.com assel_child@yahoo.com

Keywords: Electronic messages, message's symbols, Digital signature, ASCII code, QR Code #,C language

Abstract

In light of the information revolution taking place in the modern world, therefore it becomes necessary and important to save this electronic messages. So we offered this technique to ensure the safety of the content of the messages and authenticity of the sender through networks communication by converting the message's symbols to numbers , each one of this symbols (letters, numbers, symbols) will converted into three digits, the first digit represents the ASCII code of the symbol , the second digit represents the frequency of this symbol in the message (the number of times this symbol is appear in the message), and the third digit represents the total number of the locations of the symbol (calculates the symbol location from the first symbol in the message to this symbol itself and blanks also calculated too) .The digital signature of the sender will converted to numbers like the symbols of message we explained it before, and this numbers of the digital signature will gathering together to produce three numbers only, this number will gathering with each numbers of the message's symbols, the final numbers will converted to QR Code , the QR Code will placed with the message and sent to the recipient. The recipient returns the steps of the sender (produce QR Code from the received message) and compared it the received QR Codes, if it is match or not. The recipient will ensure that the content is secure, and confirms the authenticity of the sender.

أثبات صدق المحتوى واصالة المرسل للرسائل النصية بأستخدام QR code

فراس محمد اسود **ياسر علي مطني**

انتصار اسماعيل خضير **احمد احسان محمد**

جامعة ديالى, كلية التربية الاساسية

Altae13@yahoo.com ee22a12@gmail.com

Inteasar_yassin@yahoo.com assel_child@yahoo.com

الخلاصة

في ظل ثورة المعلومات التي يشهدها عالمنا الحديث,اصبحت المراسلات الالكترونية ضرورية ومن المهم حفظ هذه المعلومات المرسلة. لذلك عرضنا هذه التقنية لضمان سلامة محتوى الرسائل وأصالة المرسل عبر شبكات الاتصالات عن طريق تحويل رمز الرسالة إلى أرقام، كل واحد من رموز الرسالة (الحروف والأرقام والرموز) سوف تحول إلى ثلاثة أرقام، الرقم الأول يمثل أسكي كود الرمز، والرقم الثاني يمثل تردد هذا الرمز في الرسالة (عدد المرات التي يظهر فيها هذا الرمز في الرسالة)، والرقم الثالث يمثل العدد الإجمالي لمواقع تكرارات هذا الرمز (يحسب موقع الرمز من الرمز الأول في الرسالة إلى هذا الرمز نفسه وتحسب الفراغات أيضا). وسيتم تحويل التوقيع الرقمي للمرسل إلى أرقام مثل رموز الرسالة كما أوضحناها سابقا، هذه الأرقام للتوقيع الرقمي سوف تجمع معا لإنتاج ثلاثة أرقام فقط، وهذا الرقام الثلاثة تجمع مع أرقام رموز الرسالة ، بعدها تم تحويل هذه الأرقام إلى كيو ار كود، يوضع كيو ار كود مع الرسالة ترسال إلى المستلم. المستلم يقوم بأجراء خطوات المرسل (تكوين كيو ار كود من الرسالة المستلمة) ويتم مقارنة الكيو ار كود ما إذا كان مطابق أم لا. وسيضمن المستلم أن المحتوى آمن، ويؤكد صحة المرسل.

الكلمات المفتاحية: رسائل الكترونية, رموز الرسالة, التوقيع الرقمي, الاسكي كود, الكيو ار كود , لغة سي#.

المقدمة

يمثل أمن وسرية المعلومات حماية وتأمين الموارد المستخدمة كافة والعمل على سريتها وسالمتها , وفي غياب أمن المعلومات, أو نقصه ,أو توقفه وعدم االستفادة القصوى منه يؤدي إلى فقدان الثقة بين المرسل والمستلم . ولهذا يعد أمن المعلومات من الركائز الضرورية والحاكمة في حماية أألفراد والشركات والحكومات من الاضرار الناتجة ,ولضمان أمن المعلومات وسريتها هناك طرق دقيقة وملائمة وموثوق منها ,مثل الجدران النارية وكلمة السر والتشفير وغيرها من الطرائق التي تستخدم لعدم إفشاء البيانات والمعلومات المخزونة والمرسلة [1].

مع تعاظم دور شبكات المعلومات في عالمنا ، وازدياده حجم تبادل البيانات والمعلومات عبرها، واحتواء الشبكة على كم هائل من المعلومات الهامة جدا، أصبحت عملية حماية تلك البيانات الهامة احد أهم التحديات التي يسعى المتخصصون في مجال حماية المعلومات توفيرها. وتبين الدراسات وجود تزايد ملحوظ في عمليات اختراق تلك البيانات الهامة، مما يتطلب صياغة وتطوير طرق جديدة لحماية تلك المعلومات التي لا تقدر بثمن، وكذلك حماية وتأمين كافة المعلومات الرقمية , ومن وسائل الحماية تلك ظهور مفهوم التوقيع الرقمي Digital Signature.

الغش والخداع من الهجمات الامنية التي تواجه عملية تناقل الرسائل النصية والمستندات والوثائق عبر شبكة الانترنيت وخصوصا مؤسسات الحوكمة الالكترونية والتجارة الالكترونية والتعاملات المالية الالكترونية حيث ان الغش والخداع له عدة اوجه منها تزييف المعلومات , تحويرها , تغيير المحتوى , كذلك انكار المسؤولية بالارسال من قبل المرسل الاصلي او الادعاء بان يكون المتطفل هو الطرف المرسل المخول [2].

عناصر أمن المعلومات

السرية Confidentiality: واحدة من الطرق التي نحافظ فيها على سرية المعلومات هي بالتشفير.

التكاملية Integrity: تعبر عن كيف نقوم بتخزين البيانات ونتأكد بأنه لم يتم التعديل عليها سواء من قبل المخترقين أو حتى الأشخاص المصرح لهم بالاطلاع على البيانات. وكذلك عند نقل البيانات من مكان لمكان فهل تم اعتراض هذه البيانات والتعديل عليها؟

التوافر Availability: وهي أن تكون البيانات أو الأجهزة والشبكات متوفرة عند طلبها وعند الحاجة إليها [4].تم استخدام الباركود على نطاق واسع لتحديد اصالة المنتجات , رموز الاستجابة السريعة (كيو ار كود) تمثل ببعدين من الباركود التي يمكن ان تتضمين نص ,صوت , فيديو, عنوان على شبكة الإنترنت، ووثائق التفويض وأكثر من ذلك بكثير. تناول بعض البحوث مفهوم الكيو ار كود واستخداماتهة في ترميز الرسالئل , لقد اقترح تشفير بيانات باستخدام خوارزمية التشفير (AES). ويستند العمل تحويل الرموز المشفرة إلى كيو ار كود و من ثم باستخدام الماسح الضوئي لفك تشفيرها [5].

ان اهمية هذا البحث تكمن في الحفاظ على محتوى الرسائل واصالة المرسل لهذه الرسائل , ولاهمية هذه الرسائل التي من الممكن ان تكون سرية وذات اهمية كبيرة مثل التخاطبات الحكومية الالكترونية والمعاملات المالية والتجارية, هذه التقنية التي تم تصميمها تعمل وبشكل مثالي الى حد ما على التاكد من سلامة محتوى الرسائل المرسلة في الشبكات والاتصالات واصالة المرسل, وان الهدف من البحث هو اثبات صدق وسلامة محتوى الرسائل من التحوير والتلاعب والتزييف وكذلك اثبات اصالة المرسل , وعدم الانكار بالنسبة للمرسل المخول[3].

نقدم هنا في بحثنا هذا امكانية التاكد من سلامة محتوى الرسائل واصالة مرسلها بشكل مثالي الى حد ما, عن طريق تمثيل ثلاثة ارقام لكل رمز من رموز الرسالة ان كان حرف او رقم او رمز معين, فالرقم الاول يمثل الاسكي كود(ASCII code هو نظام ترميز من ٧ بت يستخدم سبعة أرقام ثنائية القاعدة (قيمة تتراوح بين ٠ و١٢٧) لتمثيل الحروف والارقام والرموز كما موضح في الشكل (١-١) هناك اهمية لهذا الرمز ففي حال تغير هذا الرمز بفعل متطفل فسيتغير هذا الرقم الاول, اما الرقم الثاني فيمثل تكرار هذا الرمز في الرسالة كذلك سيتغير هذا الرقم اذا تغير رمز واحد من هذه الرموز,واما الرقم الثالث وهو مهم جدا فهو يمثل مواقع تكرارات هذا الرمز في الرسالة ففي حال تم تقديم وتاخير اي رمز من رموز الرسالة سيتغير هذا الرقم.

Dec	Char	Dec	Char	Dec	Char	Dec	Char	Dec	Char	Dec	Char
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	'	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o	127	_
48	0	64	@	80	P	96	`	112	p		

الشكل (١-١)

ملاحظة هذه التقنية تدعم الرسائل باللغة الانكليزية والعربية.

خوارزمية أثبات صدق المحتوى واصالة المرسل للرسائل النصية بأستخدام QR code

اولا: من جانب المرسل

١- يقرأ نص الرسالة المراد ارسالها.

٢- يمثل كل رمز من رموز الرسالة (احرف, ارقام,رموز) بثلاث ارقام الرقم الاول يمثل الاسكي كود لهذا الرمز, والرقم الثاني يمثل تكرار هذا الرمز في الرسالة(عدد مرات تواجد هذا الرمز بالرسالة), اما الرقم الثالث فيمثل مجموع مواقع تكرارات هذا الرمز (يحسب موقع الرمز من اول رمز وصولا له والفراغات تحسب كذلك).

٣- يرمز التوقيع الرقمي (المعلوم لدي المرسل والمستلم) بنفس الطريقة في الخطوة الثانية(اي لكل رمز من رموز التوقيع الرقمي يمثل بثلاثة ارقام), ويجمع كل قيم هذه الرموز ليكون هناك ثلاثة ارقام للتوقيع الرقمي(الرقم الاول هو مجموع الاسكي كود لكل رمز من رموز التوقيع الرقمي,والرقم الثاني يمثل مجموع تكرارات رموز التوقيع الرقمي,والرقم الثالث يمثل مجموع مواقع تكرارات رموز التوقيع الرقمي).

٤- يجمع ارقام كل رمز من رموز الرسالة المراد ارسالها (الناتجة من الخطوة الثانية) مع ارقام التوقيع الرقمي(لناتجة من الخطوة الثالثة).

٥- تحول هذه القيم الناتجة في الخطوة الرابعة الى QR Code ويرفق مع الرسالة ويرسل الى المستلم.

ثانيا: من جانب المستلم

١- يقوم المستلم بتتحويل رموز الرسالة المستلمة الى QR Code كما في جانب المرسل.

٢- يطابق ال QR Code المنتج من رموز الرسالة و ال QR Code المستلم مع الرسالة.

٣- اذا كانت النتيجة مطابقة فهذا دليل على سلامة محتوى الرسالة واصالة مرسلها, اما اذا كانت النتيجة غير متطابقة فهذا دليل على ان هناك تلاعب او تزييف او تغيير في محتوى الرسالة او عدم مصداقية مرسلها.

اذا هذه التقنية تكشف اذا تم اضافة او حذف اي رمز من رموز الرسالة وتكشف كذلك اذا تم تغيير ترتيب رموز الرسالة فمثلا لو ارسل رقم (value) وتم تغيره بفعل متطفل الى (valeu) سيتم كشف هذا التغيير من خلال هذه الطريقة كما سيتبين ذلك اكثر في المراحل الاخرى من بحثنا هذا.

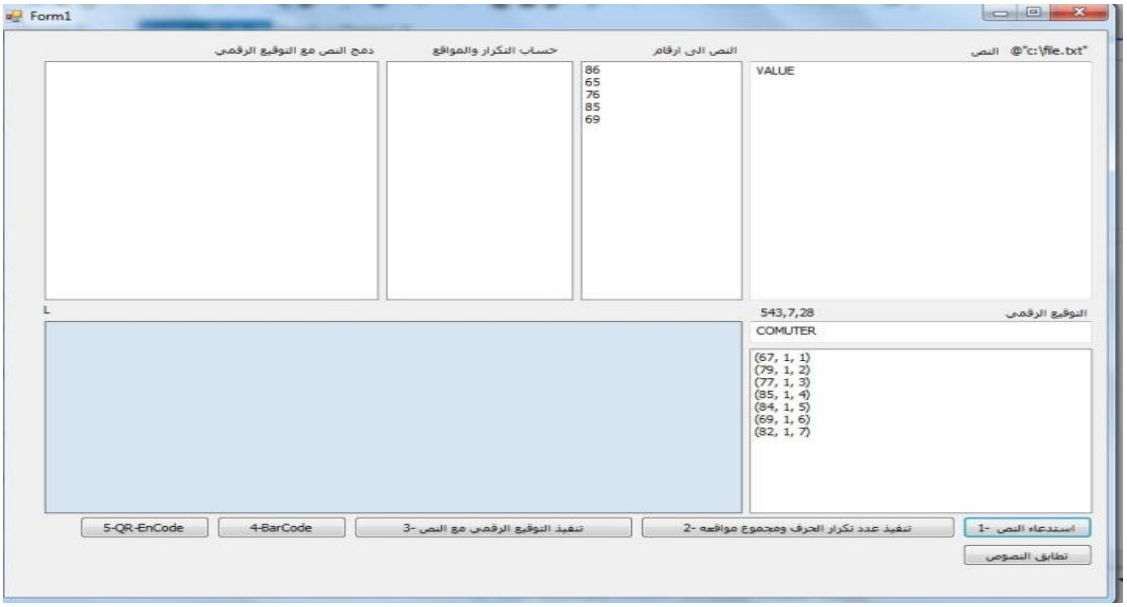
تم برمجة هذه الخوارزمية بلغة (#C) سي# (بالإنجليزية: #C) (تلفظ سي شارب) هي لغة برمجة متعددة الأنماط تتمتع بكونها سكونية التنميط وأمرية وتعريفية ووظيفية وإجرائية وعمومية وشيئية المنحى (غرضية التوجه) (باستخدام الصفوف) كما تخضع لمبادئ البرمجة التركيبية المنحى [6].

ملاحظة: كود البرمجة بلغة C# فقط.

مثال عملي

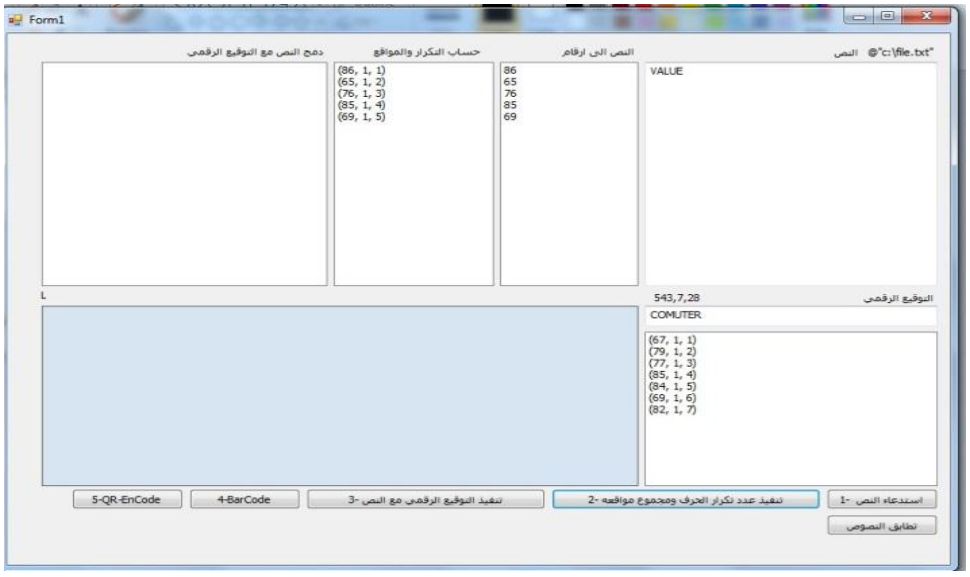
مثال عملي على ما تقدم من ذكره موضح بالصور والشرح بالتفصيل, مثل ندخل كلمة (VALUE) نكتب نص كلمة (VALUE) في المربع المخصص له ونضغط على مفتاح (استدعاء النص), حيث سيتم حساب الاسكي كود لكل حرف, وان التوقيع الرقمي هو (computer) كما في الشكل (١-٢).

حيث ان ارقام التوقيع الرقمي جمعت مع بعض وانتجت (٥٤٣,٧,٢٨) ,هذه الارقام تجمع مع كل ارقام الرمز من الرسالة , مثلا ارقام الحرف (V) هي (٦٧,١,١) تجمع مع رقم التوقيع الرقمي (٥٤٣,٧,٢٨) فينتج رقم اخر لكل رمز من رموز الرسالة ثم تحول هذه الارقام الاخيرة الى كيو ار كود.



الشكل (١-٢)

بعدها نضغط على مفتاح (تنفيذ عدد تكرار الحرف ومجموع مواقعه), حيث سيتم حساب تكرار كل حرف وحساب مجموع مواقع تكراراته كما في الشكل(١-٣)

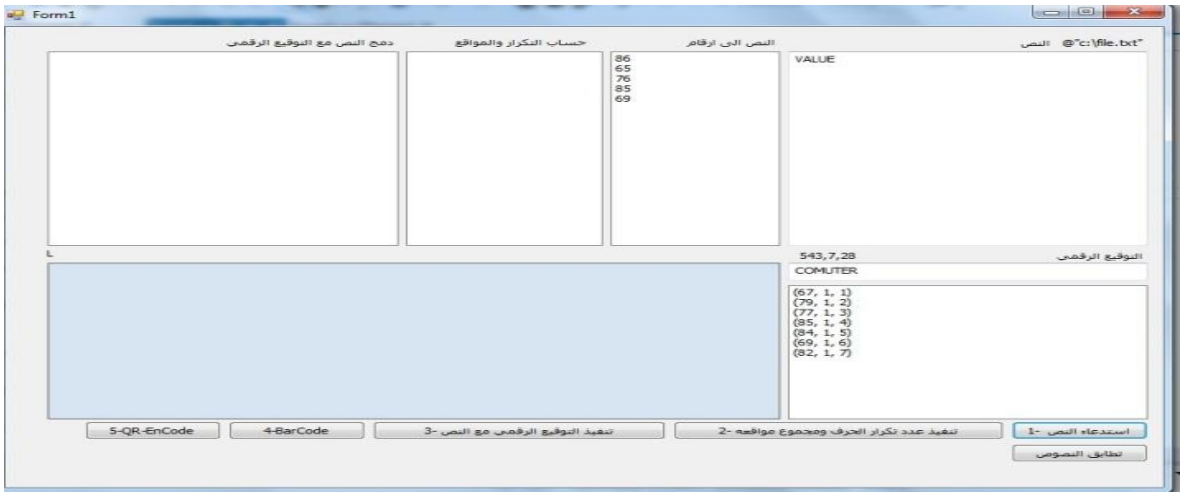


الشكل(١-٣)

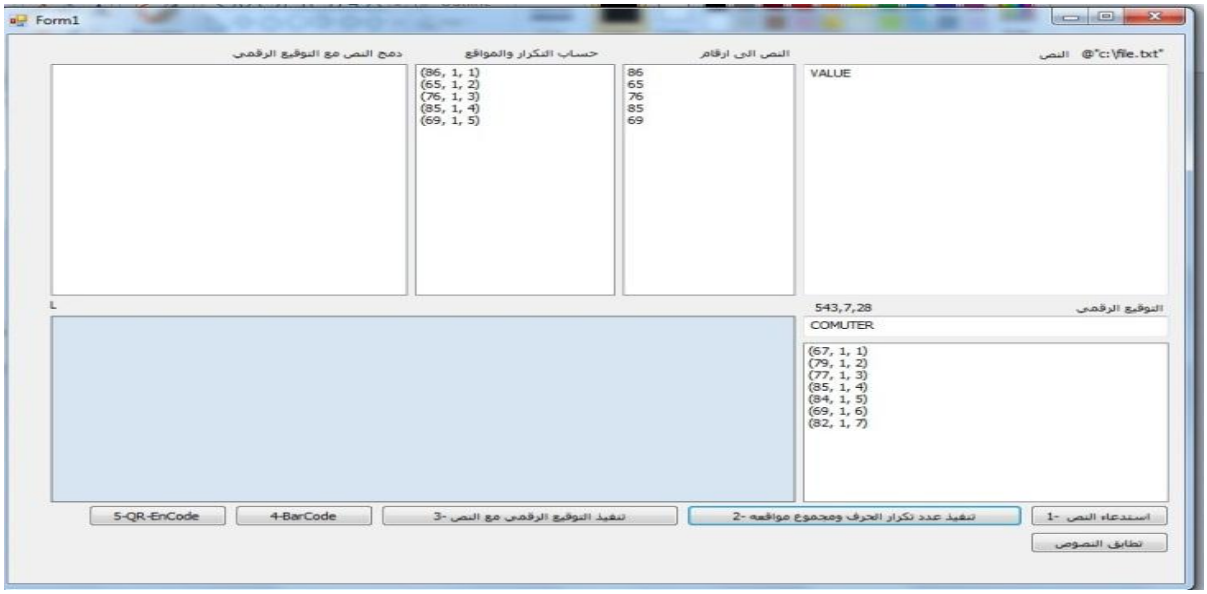
وبعد هذه الخطوة نضغط على مفتاح QR–EnCode لتكوين QR–Code خاص لهذه الكلمة المكتوبة كما في الشكل (٤–١)

الشكل (٤–١)

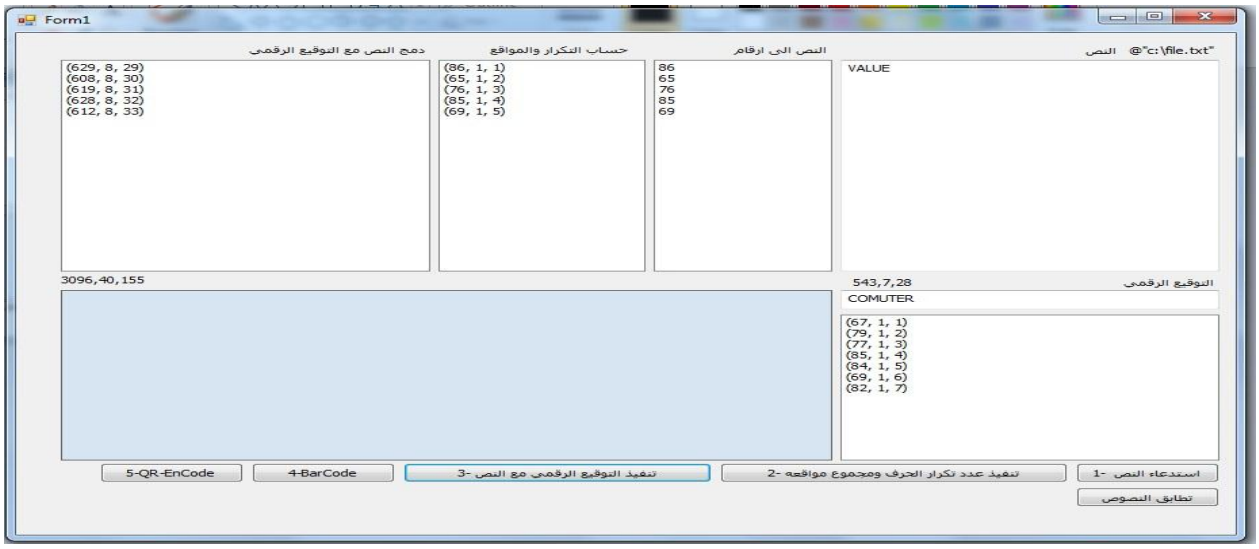
الان نعيد الخطوات السابقة ولكن بتغيير مواقع حرفين مثل (VALUE) كما في الاشكال التالية (الشكل (٥–١), الشكل (٦–١), الشكل(٧–١),والشكل (٨–١)).



الشكل (٥–١)



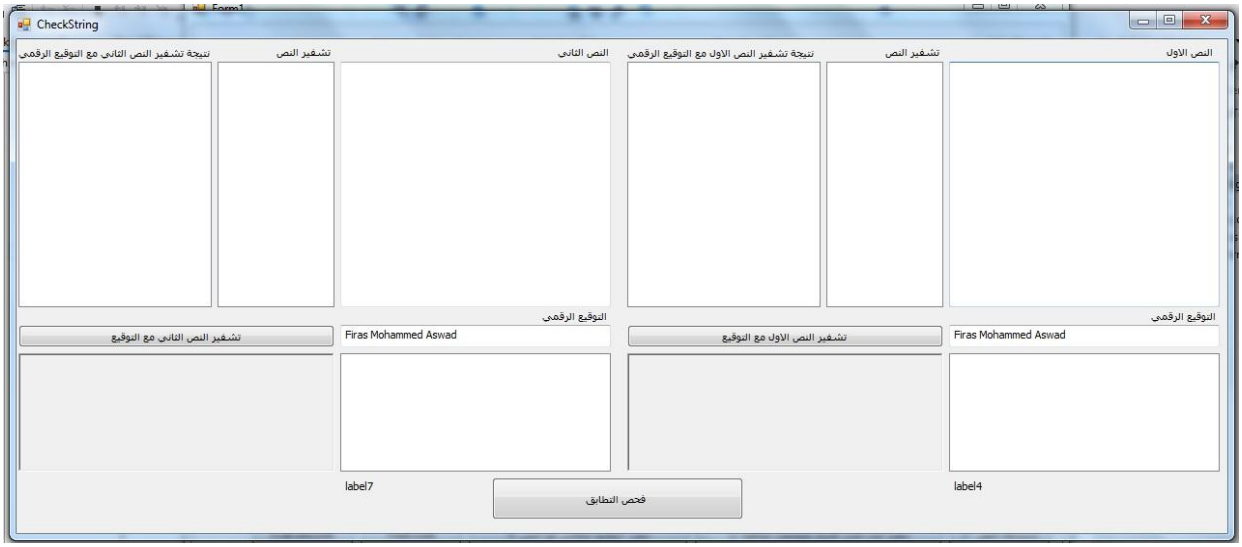
الشكل(٦-١)



الشكل(٧-١)

الشكل (٨-١)

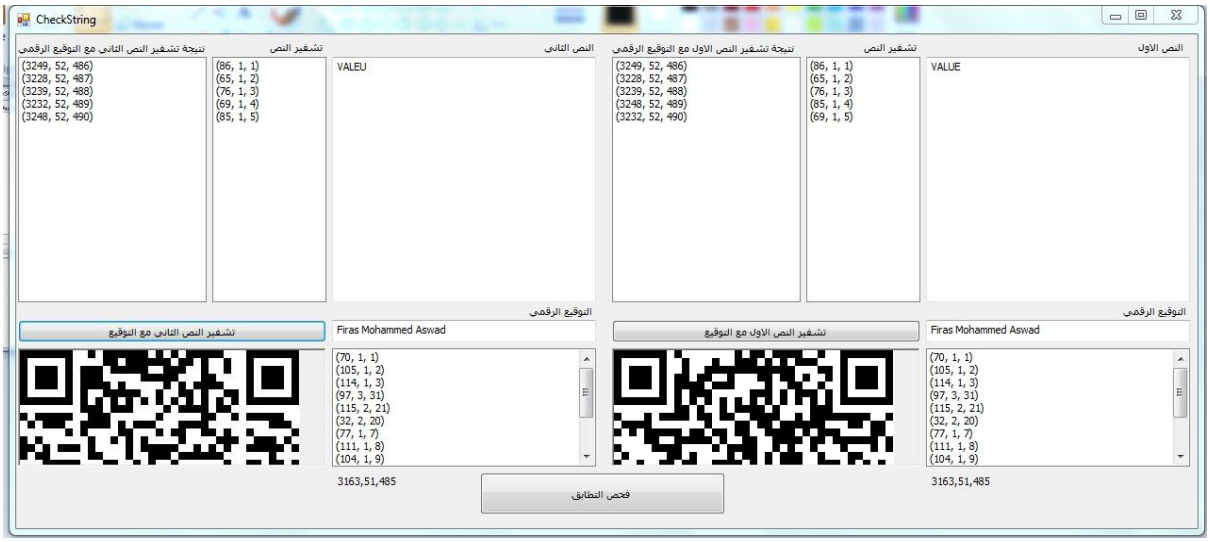
الان لو نلاحظ ان هناك قيم رقمية تغيرت مكانها ,ولاثبات ذلك نجري الخطوات التالية.مرحلة المطابقة ل QR-Code المتكون للكلمتين (VALUE) و (VALEU) كما في الاشكال التالية.



الشكل (٩-١)

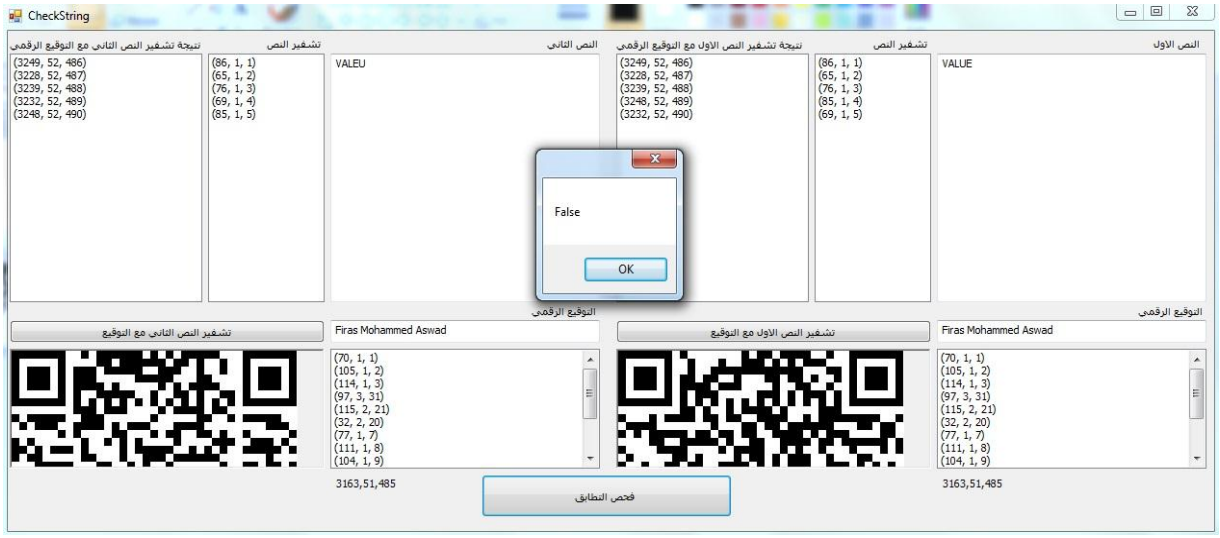
نكتب كلمة (VALUE) في مربع النص الاول , وكلمة (VALEU) في مربع النص الثاني كما في الشكل (٩-١) اعلاه.

سينتج QR-Code لكل كلمة كما موضح في الشكل (١٠-١) التالي



الشكل (١٠-١)

نضغط على مفتاح فحص التطابق وستضهر النتيجة كما في الشكل (١١-١) التالي.



الشكل (١١-١)

هنا لو نلاحظ نتيجة الفحص هي (False) بالرغم ان الاختلاف هو فقط تغيير مكان حرفين ضمن النص فقط.وهذا يثبت قوة ودقة هذه الخوارزمية المستخدمة لاثبات سلامة محتوى الرسائل واثبات اصالة المرسل عن طريق التوقيع الرقمي.هذا هو كود برنامج في لغة سي# لتحويل الارقام الى كيو ار كود

```
private string QRcodeString; public QrCodeForm(string qrcodeString)
    { this.QRcodeString = qrcodeString; InitializeComponent();}
private void QrCodeForm_Load(object sender, EventArgs e)
    { using (SaveFileDialog sfd = new SaveFileDialog() { Filter = "Jpge|*.jpg",
ValidateNames = true})
      { if (sfd.ShowDialog() == DialogResult.OK) {
MessagingToolkit.QRCode.Codec.QRCodeEncoder enCode = new
MessagingToolkit.QRCode.Codec.QRCodeEncoder();enCode.QRCodeScale = 8;
Bitmap bmp = enCode.Encode(QRcodeString); pictureBox1.Image = bmp;
bmp.Save(sfd.FileName, ImageFormat.Jpeg); }
```

هنا لو نلاحظ ان حجم الكيو ار كود المنتج من الارقام مثل برقم ٨ في الكود(enCode.QRCodeScale = 8);) حيث يمكن ان نجعلهة اكبر بتغير رقم ٨ الى رقم اكبر.

النتائج

١-هذه الطريقة الترميزية هي طريقة مثالية الى حدا ما بكشف التلاعب ان حصل في محتوى الرسائل حتى وان كان هذا التلاعب على مستوى بسيط مثل تغيير مكان رمز برمز اخر ظمن الرسالة الواحدة.

٢-التأكد من اصالة المرسلة للرسألة بأستخدام التوقيع الرقمي.

التوصيات

١-نوصي مؤسسات الحوكمة الالكترونية ,مؤسسات التجارة الالكترونية, ومؤسسات المالية الالكترونية بأعتماد هذه التقنية في مراسلاتها لمثاليتها بكشف اي خطأ او تلاعب بالرسائل وامكانياتها العالية في اثبات اصالة المرسل .

٢-نوصي الباحثين بتطوير هذه التقنية وجعلها تعمل على الرسائل غير الرسائل باللغة العربية والانكليزية.

٣-اعتماد هذه التقنية لتكون بمثابة ختم مؤسسة الكترونية يستخدم في مراسلات هذه المؤسسات.

المصادر والمراجع

1- م.د.خلود هادي الربيعي, نهاد عبد اللطيف عبد الكريم (٢٠١٣) "أمن وسرية المعلومات وأثرها على الاداء التنافسي دراسة تطبيقية في شركتي التأمين العراقية العامة و الحمراء للتأمين الاهلية **,"** مجلة دراسات محاسبية و مالية صفحة (٥-٦).

٢-أ.د.علاء حسين الحمامي, د.محمد علاء الحمامي(٢٠٠٧), تكنلوجيا امنية المعلومات وانظمة الحماية,الطبعة الاولى, دار وائل للنشر صفحة (٤-٧).

٣-أ.د.علاء حسين الحمامي, د.محمد علاء الحمامي(٢٠٠٨),الكتابة المخفية والعلامات المائية,مكتبة الجامعة الشارقة صفحة (٣-٦).

٤- د. خالد , د.هاشم (٢٠٠٩) ,أمن المعلومات بلغة ميسرة, مكتبة الملك فهد الوطنية صفحة (١٣-٢٠).

5- Partiksha M., Nitin I. "A desktop application of QR code for data security and authentication Computation Technologies (ICICT), International Conference on (2016) page (1-2).

6- تعريف لغة C# متاح على هذا الرابط
https://ar.wikipedia.org/wiki/%D8%B3%D9%8A_%D8%B4%D8%A7%D8%B1%D8%A8