المجلة العراقية للعلوم الاحصائية (12) 2007
ص ص [245-268]

الوثوقية في الصور الرقمية

ياسين حكمت إسماعيل*

المستخلص

الهدف من هذا البحث هو تقديم طريقة مقترحة لتحقيق الوثوقية في الصور الرقمية. ولتحقيق الوثوقية في الصور الرقمية أعتمدنا على أفكار دالة التمويه أحادية الأتجاه، ملخص الرسالة، كذلك فكرة التوقيع الرقمي. تم تقديم طريقة ذات كفاءة لتحقيق العلامات المائية الرقمية (Digital Watermarking) في الصور الرقمية. وهذا العمل يدمج بين وثوقية المستخدم ووثوقية الصورة الرقمية، ومن ثم بأمكان مستلم الصورة الرقمية التأكد من وثوقية الصورة ووثوقية الجهة المرسلة. الهدف من هذا البحث هو الكشف عن أي تغيير في الصورة ممكن أن يحدث من قبل المتطفل في أثناء أرسالها عبر شبكة الحاسبات .

Authentication in Digital Images

Abstract

The aim of this research is to produce a proposed method for digital image authentication . To provide digital image authentication we depending on the ideas of one way hash function , message digest , and digital signature . An efficient method for digital image watermarking was suggested . This work combines between user authentication and digital image authentication , so that it allows the receiver of a digital image to be confident of both that the digital image is authentic and it is delivered from authorized source . The goal of this research

* مدرس مساعد/ قسم علوم الحاسبات/ كلية علوم الحاسبات والرياضيات/جامعة الموصل.

تاريخ التسلم : 19/ 6 /2006 ـــــــــــــــــــــــــ تاريخ القبول : 6/ 12 /2006

is to detect any intrusion modification on the digital image while sending through computer networks .

1. المقدمة :

أن مفهوم الوثوقية (Authentication) هو التأكد من أن الاتصال ضمن شبكة الحاسبات موثوق به . هنالك نوعان من الوثوقية هما وثوقية المستخدم ووثوقية الرسالة . تتضمن وثوقية المستخدم قابلية تحديد مستلم الرسالة (البيانات) من تحديد مدى وثوقية الجهة المرسلة ، في حين أن وثوقية الرسالة تتضمن قابلية المستلم من تحديد مدى وثوقية البيانات المرسلة أي التأكد من سلامة البيانات وأنها لم تتعرض لأي تغيير أثناء أنتقالها ضمن شبكة الحاسبات [Jan C. ,1998] [Barnes C. ,2002] [Seberry J. ,1989] . يتم ايجاد وثوقية الصورة من خلال حساب ملخص الرسالة (Massage Digest) للصورة وهي بصمة رقمية يتم أشتقاقها وفقا" لخوارزميات دوال أو أقترانات التمويه (Hash Functions) إذ تطبق هذه الخوارزميات حسابات رياضية على الصورة لتوليد بصمة صغيرة (سلسلة بيانات) ذات طول ثابت . بأمكان هذه البصمة تمييز الصورة الأصلية والتعرف عليها بدقة حتى أن أي تغيير في الصورة – ولو كان في رقم ثنائي (Bit) واحد– سيفضي إلى بصمة مختلفة ، ومن غير الممكن أشتقاق البصمة ذاتها من رسالتين مختلفتين [Schneier B. ,1996] [Stallings W.,1999]. أما التوقيع الرقمي (Digital Signature) فينتج من تشفير قيمة ملخص الرسالة. تتم أضافة التوقيع الرقمي الى الصورة لأثبات هوية مرسلها وضمان سلامة محتوياتها [Stallings W. ,1999]

[Barnes C. ,2002] . وتتم عملية إضافة التوقيع الرقمي إلى الصورة من خلال استخدام تقنية العلامة المائية الرقمية (Digital Watermarking) التي تستخدم لأثبات حقوق الملكية (Intellectual Property) أو لضمان الوثوقية . تضمن البحث تقديم طريقة مقترحة في حساب ملخص الرسالة للصورة الرقمية وبالاعتماد على فكرة دوال التمويه أحادية الاتجاه (One Way Hash

Function) . بعد ذلك تم إجراء عملية التشفير لقيمة ملخص الرسالة مع رمز خاص بالمرسل للحصول على قيمة معينة للتوقيع الرقمي. ان قيمة التوقيع الرقمي الناتجة تكون ذات كفاية اذ تستخدم بدقة في تحقيق الوثوقية لكل من الجهة المرسلة والصورة ومن ثم فأن أي تغيير في محتوى الصورة (بصورة متعمدة أو غير متعمدة) سوف يتم كشفه . طور البحث طريقة مقترحة لتقنية العلامة المائية الرقمية من خلالها يتم أخفاء قيمة التوقيع الرقمي في الصورة قبل إرسالها . وفرت الطريقة المقترحة مستوى عالياً من الوثوقية كذلك دمجت بين وثوقية الصورة الرقمية مع وثوقية الجهة المرسلة .

2. أستخدام العلامة المائية الرقمية لتحقيق الوثوقية : تتضمن آلية العلامات المائية الرقمية أخفاء بيانات قليلة نسبيا" ضمن بيانات أخرى (كوسط ناقل) ، أي لدينا بيانات والمراد طمرها داخل وسائط أخرى (ملفات نصية، صورية، صوتية). هنالك العديد من الأمثلة عن أستخدام تقنية العلامات المائية منها معلومات حق الاستنساخ (Copyright Information) ، توقيع المؤلفين الرقمي (Digital Authors Signature) ، توثيق الشركة (Company Logo) وكلها وسائل تمثل شرعية المالك [الصميدعي عامر ،2002] [Johnson N. 2001,] . هنالك العديد من الطرائق والدراسات السابقة في مجال استخدام العلامة المائية الرقمية لتحقيق الوثوقية في الصور الرقمية ، أعتمدت أولى الطرائق على حشر قيمة فحص المجموع (Check Sum) في الأرقام الثنائية الأقل أهمية ((Least Significant Bits (LSB) للبيانات التي تمثل قيم الوحدات الصورية (Pixels) للصورة ، هذا الأسلوب أعتمد عليه العالم Walton [Walton S.,1995] اذ تضمنت طريقته أختيار مجاميع شبه عشوائية من نقاط الصورة وبالأعتماد على مفتاح سري يتم أيجاد قيمة فحص المجموع للنقاط المختارة وحشر تلك القيم في الأرقام الثنائية الأقل أهمية لنقاط الصورة . أستخدم كل من Fridrich and Goljan [Fridrich J.,1999] أسلوباً جديداً فقد تم أخفاء الصورة في نفسها بهدف تحقيق الوثوقية لمحتويات الصورة وحمايتها . الطريقة أعتمدت على أخفاء نسخة مكبوسة من الصورة ضمن الصورة الأصلية

والمراد تحقيق الوثوقية لها وبنفس الأسلوب السابق فقد تم الإخفاء بالأعتماد على الرقم الثنائي الأقل أهمية لبيانات الصورة ، توفر هذه الطريقة أمكانية أصلاح أو أسترجاع جزئي لمناطق الصورة التي حدث لها التغيير أو التشويه . كما اقترح Wolfgang and Delp [Wolfgang R.,1996] [DelpE.,1999] تقنية أخرى تدعى تقنية العلامة المائية المتغيرة ذات البعدين (Variable_Watermark Two-dimensional Technique) ومبدأ عملها هو تقسيم الصورة إلى مقاطع (Blocks) بأبعاد 64*64 نقطة ويتم حشر قيمة العلامة المائية ضمن كل مقطع . للتحقق من وثوقية الصورة وتكاملها، وثم تم فحص وجود قيمة العلامة المائية أو غياب ها في كل مقطع من مقاطع الصورة، اذ أن عدم وجود قيمة العلامة المائية ضمن مقطع الصورة يعني حدوث تغيير أوتلاعب ضمن بيانات ذلك المقطع من الصورة. وقد تم أستخلاص الخواص (Features Extraction) [Dugelay J.,1999] [Rey C.,2000] من الطرائق التي تم الاعتماد عليها لتحقيق وثوقية الصورة الرقمية، اذ يتم استخلاص مجموعة من الخواص للصورة الأصلية ومن ثم أخفاء تلك الخواص ضمن بيانات الصورة . لمعرفة وثوقية الصورة تتم مقارنة خواص الصورة المستلمة مع قيم الخواص التي يتم أشتقاقها من قيمة العلامة المائية المخفية في الصورة المستلمة فإذا تساوت القيمتان دل ذلك على أن الصورة موثوق بها. قدم العالم Friedman [Friedman G.,1993] [Friedman G.,1996] طريقة لتحقيق وثوقية الصورة الرقمية تضمنت الطريقة أخفاء قيمة العلامة المائية ضمن حقول ترويسة ملف الصورة (Image File Header) . من مساوىء هذه الطريقة أنه إذا تم تغيير صيغة ملف الصورة (Format) إلى صيغة أخرى قد لا تحتوي على نفس الحقول (Fields) التي تم استخدامها لإخفاء قيمة العلامة المائية عندها سوف يتم فقدان قيمة العلامة المائية وبالاتي عدم أمكانية التحقق من وثوقية الصورة . وثمة طريقة أخرى لتحقيق الوثوقية تضمنت حساب قيمة فحص المجموع للصورة ومن ثم إرسال الصورة الأصلية لوحدها ومن ثم إرسال قيمة فحص المجموع ، عند الجهة المستلمة يتم حساب قيمة فحص

المجموع للصورة المستلمة ومقارنتها مع قيمة فحص المجموع المستلمة فاذا تطابقت القيمتان دل ذلك على أن الصورة موثوق بها.

يتضمن أسلوب العلامة المائية الرقمية المستخدم في بحثنا هذا أخفاء قيمة التوقيع الرقمي ضمن الصورة المراد تحقيق الوثوقية لها . أن آلية استخدام التواقيع الرقمية في تحقيق الوثوقية تتضمن حساب قيمة التوقيع للبيانات عند الجهة المرسلة ثم أخفاء قيمة التوقيع ضمن تلك البيانات ومن ثم إرسال البيانات وبضمنها قيمة التوقيع ، عند الجهة المستلمة يتم استخراج قيمة التوقيع من البيانات المرسلة، وفي هذه المرحلة تعود البيانات إلى صيغتها الأصلية قبل حساب قيمة التوقيع عند الجهة المرسلة، اذ يتم الآن مرة أخرى حساب قيمة التوقيع الرقمي للبيانات عند الجهة المستلمة وباستخدام نفس الخوارزميات المستخدمة عند الجهة المرسلة ، فأذا تساوت قيمة التوقيع الرقمي للبيانات والمحسوبة عند الجهة المستلمة مع قيمة التوقيع الرقمي المستخرجة من البيانات المرسلة فأن البيانات موثوق بها [Stallings W.,1999] [Barnes C.,2002].

مما سبق نجد أن استخدام مفهوم التوقيع الرقمي لتحقيق الوثوقية في الصور الرقمية يوجب ضرورة حصول الجهة المستلمة على نفس الصورة الرقمية بالضبط والتي تم حساب قيمة التوقيع الرقمي لها عند الجهة المرسلة ، وهذا غير ممكن أذ أن معظم طرائق العلامة المائية الرقمية تستخدم الأرقام الثنائية الأقل أهمية أو غيرها من الوسائل لخزن قيمة العلامة المائية الرقمية .

من هنا برزت الحاجة إلى تقديم فكرة تتضمن أمكانية أخفاء أو تضمين قيمة العلامة المائية الرقمية في الصورة بحيث عند سحب القيم المخفية في الصورة فبالإمكان إرجاع الصورة إلى وضعها الأصلي قبل عملية الإخفاء . تضمنت الطريقة المقترحة في بحثنا هذا أضافة سطر جديد في أسفل الصورة الرقمية ، هذا السطر المضاف يستخدم لأخفاء قيمة العلامة المائية ودون التأثير في بقية أجزاء الصورة . عند الجهة المستلمة يتم أستخراج قيمة العلامة المائية (التوقيع الرقمي) من السطر الأخير بعدها يتم حذف السطر المضاف حيث تعود الصورة إلى وضعها الأصلي تماما" ، ومن ثم يتم حساب قيمة التوقيع الرقمي

للصورة وأجراء المقارنة بين التوقيع الرقمي المحسوب عند الجهة المستلمة مع قيمة التوقيع المرسل والمحسوب عند الجهة المرسلة فأذا تساوت القيمتان دل ذلك على أن الصورة موثوق بها ولم يحدث لها أي تغيير أثناء أنتقالها عبر شبكة الحاسبات . وأخيرا" تجدر الإشارة إلى أن الطريقة المقترحة في بحثنا تضمنت أيضا" أجراء عملية معالجة للسطر المضاف وإعطائه قيم لونية متقاربة مع الأسطر المجاورة له وبحيث جعلت السطر المضاف منسجما" مع بقية أجزاء الصورة وأيضا" قضت على مشكلة المساحات اللونية المستوية والتي قد تظهر بالصورة ، وبالاتي جعلت من الصعوبة على المتطفل أو الشخص غير المخول من الاعتقاد بوجود سطر مضاف في أسفل الصورة .

3. مقدمة عن الصور الرقمية :

الصورة هي بيانات رقمية ذات صيغة محددة وهذه البيانات تمثل معلومات عن الصورة فضلا عن القيم اللونية للنقاط المكونة للصورة . يتم تمثيل الصورة الرقمية في الحاسوب كمصفوفة ثنائية الأبعاد (2-dimensional array) من القيم الرقمية التي تمثل كل منها شدة الأضاءة لوحدة صورية (Pixel) ، هذه القيم يستخدمها ماسح الصورة Raster لعرض اللون على الشاشة في الموقع الذي تمثله كل قيمة من هذه القيم . أن عملية الوصول الى قيم الوحدات الضوئية من قبل الماسح تعتمد على التقنية التي تم بموجبها تمثيل هذه الوحدات ، وهذا بدوره يعتمد على عدد الخلايا الثنائية المستخدمة لتمثيل كل وحدة. هنالك ثلاثة أنواع للصور الرقمية وهي [العريبي علياء ،2003] [Scott E. ,1998]
[Gonzales ,2002] [Demuth H. ,1998] [Jain A. , 1998] :

أ. الصور الثنائية : تمثل الصور الثنائية أبسط أنواع الصور الرقميـــة اذ ان كل وحدة صورية تكون قيمتها (0 أو 1) . تخزن الصور الثنائيـــة كمصـــفوفة ثنائية الأبعاد من الأصفار والواحدات . في هذا النوع من الصور هنالك لونـــان فقط ، ولهذا سميت بالصور الثنائية .

ب. الصور ذات التدرج الرمادي : الألوان في هذا النوع من الصور هي ظلال من التدرج الرمادي . الصورة ذات التدرج الرمادي هي صورة أحادية اللون أيضا" لكنها تتكون من ظلال من التدرجات الرمادية تعطي معلومات عن شدة الإضاءة فقط دون اللون . اللون الرمادي ينتج عندما تكون قيم الشدة للألوان الأحمر ، الأخضر ، الأزرق متساوية في فضاء الـ RGB . يعتمد عدد الألوان في هذا النوع من الصور على عدد الأرقام الثنائية المستخدمة لتمثيل الوحدة الصورية . أن عدد الأرقام الثنائية المستخدمة في تمثيل الوحدة الصورية في الصور ذات التدرج الرمادي هي 8,6,4 ومن ثم فأن عدد الألوان هو : $2^{\text{عدد الأرقام الثنائية}}$ أي 256,64,16 لون .

ج. الصور الملونة : هناك مجموعة من الألوان تدركها العين البشرية والتي تنتج ببساطة بإضافة كميات مناسبة من الأحمر الأخضر والأزرق . هذه الألوان تعرف بالألوان الأساسية ومن الممكن تكوين كل الألوان المرئية بتجميع هذه الألوان الثلاثة . إن ظاهرة الألوان الأساسية تنتج في الحقيقة بان العين البشرية تملك ثلاثة أنواع مختلفة من مستقبلات الألوان في شبكية العين لكل نوع من الألوان القابلية على تحسس أحد الألوان الأساسية . يمكن تمثيل الصور الرقمية الملونة بتخصيص قيم الشدة منفصلة لمحتويات الألوان الرئيسية الثلاثة إذ إن اللون لكل نقطة ضوئية يحدد من خلال تجميع الألوان الأساسية الثلاثة الأحمر Read الأخضر Green الأزرق Blue وبدمج شدات الإضاءة لهذه الألوان الثلاثة يتم تشكيل اللون المطلوب (RGB) . كما هو الحال في الصور ذات التدرج الرمادي فأن عدد الألوان في الصور الملونة يعتمد أيضا" على عدد الأرقام الثنائية المستخدمة في تمثيل الوحدة الصورية . أن عدد الأرقام الثنائية المستخدمة في تمثيل الوحدة الصورية في الصور الملونة هو 32,24,16,8 وهكذا فأن عدد الألوان في الصور الملونة هو : $2^{\text{عدد الأرقام الثنائية}}$.

4. وصف موجز لملفات الصور الرقمية نوع BMP :

في الجانب العملي للبحث تم اختيار ملف الصور (BMP) الذي اعدته شركة (Microsoft) ، لكون هذا النوع من ملفات الصور يمثل الصيغة القياسية للنوافذ (Windows) ، اذ يقوم بخزن نماذج الصورة بصيغة غير معتمدة على نوع أجهزة العرض (Hardware Device) ، كذلك فأن الصور في هذا التشكيل (Format) لا تحتوي على أي نوع من أنواع المعالجة مما يوفر مساحة أخفاء أكبر . الجدول (1) يوضح الصيغة القياسية لمحتويات الملف لهذا النوع من التشكيل .

الجدول (1) يوضح مكونات ملف الصورة نوع (BMP)

الحقول	عدد الكلمات الثنائية (Bytes)	البيانات	الوصف
ترويسة ملف الـBMP			
1	2-1	نوع الملف	يجب أن يكون بصيغة ASCII وتكون قيمته "BM"
2	6-3	حجم الملف	يخصص 32 رقماً ثنائياً لتمثيل حجم الملف
3	10-7	محجوزة للاستخدام المستقبلي	يجب أن تكون قيمتها صفر
4	14-11	قيمة الـ offset لملف BMP	تمثل البداية لملف الصورة
معلومات ملف الـBMP			
5	18–15	عدد الكلمات الثنائية في جزء الترويسة	حاليا" 40 كلمة ثنائية
6	22–19	عرض صورة الـ Bmp	العرض مقاس بالنقطة Pixel
7	26–23	ارتفاع صورة الـ Bmp	الارتفاع مقاس بالنقطة Pixel

8	28-27	عدد مستويات الصورة	يجب أن تكون قيمته 1
9	30-29	عدد الأرقام الثنائية في كل نقطة	الاختيارات المسموحة هي 24,8,4,1
10	34-31	نوع الكبس	0 : بدون كبس ، 1 : 8 بت في كل نقطة ، 2 : 4 بت في كل نقطة
11	38-35	حجم الصورة	مقاس بالكلمات الثنائية
12	42-39	الدقة الأفقية للصورة	مقاسة بـــ Meter/Pixel
13	46-43	الدقة العمودية للصورة	مقاسة بـــ Meter/Pixel
14	50-47	عدد فهرسة الألوان المستخدمة	القيمة صفر توضح أن كل الألوان ضرورية
15	54-51	عدد فهرسة الألوان الضرورية	القيمة صفر توضح أن كل الألوان ضرورية
لوحة الألوان Palette (indexes)			
16	4*عدد الفهارس	قيمة اللون الـــRGB	الفهارس (0 ، 2 ، أو 256)
النماذج Samples			
17	حجم النماذج	قيمة النماذج	Mono : رقم ثنائي واحد 256 : كلمة ثنائية واحدة True : 3 كلمات ثنائية

يتألف الملف (BMP) من الأجزاء الرئيسية الأربعة الاتية :

الجزء الأول : بادئة الملف التي تحدد نوع الملف (BMP) ، حجمه ، منطقة محجوزة ، ثم عدد من الكتل الثمانية لحين الوصول إلى بداية نموذج الصورة .

الجزء الثاني : معلومات ضرورية عن الصورة أهمها أبعاد الصورة ، عدد الخلايا الثنائية المستخدمة لكل نموذج صوري ، حجم ملف الصورة .

الجزء الثالث : فيه جدول تواجدات الألوان (Index) أو ما يطلق عليه لوحة الألوان (Palette) ، اذ يمثل كل مدخل فيه بأربع كتل ثمانية كل كتلة تقابل لونا"

من الألوان الرئيسية الثلاثة الأزرق ، الأخضر ، والأحمر أما الكتلة الرابعة فمتروكة للاستخدامات المستقبلية (Reserved). أما عدد المداخل في هذا الجزء فتعتمد على نوع التمثيل لنموذج الصورة . فالصورة ذات التمثيل (24 رقماً ثنائياً لكل نقطة) 24 خلية لا تحتوي على هذا الجزء لكون نماذج الصورة تمثل اللون الحقيقي (True Color) ، وفي الصورة ذات التمثيل الثماني (8 ارقام ثنائية لكل نقطة) فأن حجم هذا الجزء (1024) كتلة ثمانية لاحتوائه على (256) مدخلاً (255–0) . الصور ذات التمثيل الأحادي (رقم ثنائي واحد لكل نقطة) فتحتوي على مدخلين فقط ، الأول فيه القيمة 00 للكتل الثلاثة التي تمثل اللون الأسود أما المدخل الثاني ففيه القيمة (255) للكتل الثلاثة والتي تمثل اللون الأبيض ، في حين أن الصور ذات التمثيل (4 ارقام ثنائية لكل نقطة) فأن لوحة الألوان تتكون من 16 أدخالاً كل أدخال يمثل تدرجا لونيا معينا اذ يتم تمثيل كل 4 أرقام ثنائية كعنوان الإدخال في لوحة الألوان والذي يحدد اللون الذي تتكون منه النقطة . وتجدر الإشارة إلى أن الصور ذات التمثيل (32 رقما ثنائياً لكل نقطة) فهي شبيهة بنوع الصور ذات التمثيل 24 خلية أي لا تحتوي على هذا الجزء والاختلاف أن تمثيل كل نقطة بأربع كلمات ثنائية ، أول ثلاث كلمات تمثل القيمة اللونية للنقطة (RGB) والكلمة الثنائية الأخيرة تمثل شدة الإضاءة (Intensity) للنقطة (Pixel) .

<u>الجزء الرابع</u> : هذا الجزء خاص بنماذج الصورة والتي سوف يتم أستخدامها لتحقيق عملية الأخفاء ، لذلك سوف يتم تجاوز الأجزاء الثلاثة السابقة عند التطبيق الأخفاء (العلامات المائية الرقمية) وصولا" الى هذا الجزء . [الصميدعي عامر ،2002] [العريبي علياء ،2003]
[Brown W. , 1995] [Jain A. , 1998] [Demuth H. ,1998]

5. الجانب العملي للبحث : تضمن الجانب العملي للبحث تقديم الخوارزميات المقترحة الاتية : أولا" : خوارزمية تحقيق الوثوقية في الصور الرقمية يتم تنفيذها عند الجهة المرسلة .

ثانيا" : خوارزمية تغيير القيم اللونية في السطر المضاف ويتم تنفيذها أيضا عند الجهة المرسلة.

ثالثا" : خوارزمية التحقق من وثوقية الصورة المستلمة ويتم تنفيذها عند الجهة المستلمة .

أولا" : خوارزمية تحقيق الوثوقية :

1. فتح ملف الصورة المراد تحقيق الوثوقية لها وبأي تمثيل كان (32,24,16,8,4,1 رقم ثنائي لكل نقطة) .

2. فحص أبعاد الصورة (العرض ، الارتفاع) اذ أن الخوارزمية المقترحة تفرض أن تكون أبعاد الصورة الرقمية والمراد تحقيق الوثوقية لها بالأبعاد الاتية:

العرض =>42 ، الارتفاع=>4 ، وتعتبر الصورة بهذه الأبعاد صغيرة نسبيا" .

3. أيجاد وثوقية الصورة المتضمنة ألاعتماد على فكرة دالة التمويه أحادية الأتجاه والحصول على ملخص الرسالة . تتضمن عملية أيجاد وثوقية الصورة الخطوات الاتية :

أ. يتم تقسيم الصورة (جزء البيانات (Data)) وبالأعتماد على عدد النقاط إلى جزأين متساويين وكما موضح في الشكل (1) .

ب. ناتج عملية XOR بين جميع الكلمات الثنائية (بالأعتماد على نوع التمثيل) للنقطة الأخيرة في الصورة تعطى كقيمة أبتدائية للمتغير ID-image والذي يمثل قيمة وثوقية الصورة .

ج. أن عملية أجراء XOR بين قيم النقاط (جزء البيانات في الصورة) تعتمد على نوع التمثيل المستخدم لتمثيل النقطة وتشمل الحالات الاتية :

أ. 1،4،8 ارقام ثنائية لكل نقطة : في هذه الأنواع من التمثيل فأن كل نقطة يتم تمثيلها على الأكثر بكلمة ثنائية واحدة . اذ يتم عمل XOR بين الكلمة الثنائية الأولى (النقطة الأولى) في الجزء الأول من الصورة مع الكلمة الثنائية الأولى في الجزء الثاني من الصورة وهكذا . ومن ثم أجراء عملية الـXOR بين القيم الناتجة للحصول على كلمة ثنائية واحدة تمثل وثوقية الصورة .

ب. 16 رقماً ثنائياً لكل نقطة : في هذا النوع من التمثيل فان كل نقطة في الصورة يتم تمثيلها بكلمتين ثنائيتين . اذ يتم عمل XOR للكلمة الثنائية الأولى ضمن النقطة الأولى في الجزء الأول مع الكلمة الثنائية الأولى ضمن النقطة الأولى في الجزء الثاني ثم الكلمة الثنائية الأولى ضمن النقطة الثانية في الجزء الأول مع الكلمة الثنائية الأولى ضمن النقطة الثانية في الجزء الثاني وهكذا إلى نهاية الصورة . القيمة الناتجة للـ ID-Image كأنما تمثل القيمة الابتدائية ثم يتم الرجوع إلى الكلمة الثنائية الثانية في كل نقطة وأجراء عملية الـ XOR بينها وبنفس الأسلوب المتبع في أعلاه .

ج. 24 رقماً ثنائياً لكل نقطة : في هذا النوع من التمثيل فان كل نقطة في الصورة يتم تمثيلها بثلاث كلمات ثنائية ، ولأجراء عملية الـ XOR يتم عمل XOR للكلمة الثنائية الأولى في جميع النقاط في الصورة وقيمة الـ ID-Image الناتجة تعتبر كقيمة أبتدائية ثم عمل XOR للكلمة الثنائية الثانية ثم الكلمة الثنائية الثالثة .

ء. 32 رقماً ثنائياً لكل نقطة : في هذا النوع من التمثيل فأن كل نقطة يتم تمثيلها بأربع كلمات ثنائية ، وللحصول على وثوقية الصورة يتم حساب ناتج الـ XOR للكلمة الثنائية الأولى ، الثانية ، الثالثة ، ثم الرابعة ولجميع النقاط في الصورة .

Byte1	Byte2	Byte3	.....
Part 1			n
Byte1	Byte2	Byte3	.....
Part 2			nn

ID-Image = part 1(1) XOR part 2 (1)

ID-Image = ID-Image XOR [part 1(2) XOR part 2 (2)]

ID-Image = ID-Image XOR [part1 (n) XOR part 2 (nn)]

الشكل (1) تقسيم جزء البيانات للصورة لحساب وثوقيتها

4. أدخال الـ ID-User ويكون حجمه أربع أحرف (أربعة كلمات ثنائية) هذه القيمة تستخدم لتحقيق وثوقية المستخدم (User Authentication) . يتم أخفاء قيمة الـ ID-User بعد تشفيره مع قيمة وثوقية الصورة ID-Image (الحصول على قيمة التوقيع الرقمي)ضمن جزء البيانات للصورة (في السطر الذي سوف تتم أضافته أسفل الصورة) . عند الجهة المستلمة يتم استخراج قيمة الـ ID-User والبحث عنه ضمن قاعدة البيانات لمعرفة وثوقية الجهة المرسلة .

5. توليد مفتاح (Key) حجمه 8 كلمات ثنائية بالأعتماد على بيانات الصورة وقيم ثابتة تستخدم في الخوارزمية وهي Key-b=64 , Key-a=127 . أن المفتاح الناتج يستخدم لتحقيق مستوى عال من السرية لقيم الـ ID-User و الـ ID-Image ومن ثم الحصول على توقيع رقمي عالي المستوى من السرية ، أن عملية توليد المفتاح يمكن تلخيصها بالخطوات الاتية :

أ. توحيد التمثيل لقيم النقاط في الصورة بكلمة ثنائية واحدة لكل نقطة في الصورة وذلك بعمل XOR لقيم الأرقام الثنائية التي تمثل النقاط في الصورة ، أي تحويل أنواع التمثيل 16،24،32 رقماً ثنائياً لكل نقطة الى 8 أرقام ثنائية لكل نقطة (كلمة ثنائية لكل نقطة) اذ يتم الحصول على مصفوفة جديدة تمثل بيانات الصورة تسمى array .

ب. أعطاء قيم ابتدائية للمتغيرات الاتية :

Row-length = Image width
Start=(Row-length+Key-b+Key-a)Mod(Row-length XOR array (Start))

اذ أن المتغير Start يستخدم كمؤشر (Pointer) الى عناوين ومحتويات المواقع ضمن المصفوفة array .

ج. توليد مصفوفة جديدة أسمها Filter حيث :

Size (Filter) = Size (Key-b) =127

ء. توليد مصفوفة جديدة أسمها array2 حيث :

Array2 = Filter XOR array

هـ. أعطاء قيمة جديدة للمتغير Start حيث :

Start =(Row-length+1981+Key-b)Mod(Row-length XOR array (Key-a))

و. بالأعتماد على قيمة المتغير Start الجديدة وقيمة المصفوفة array2 يتم الحصول على مفتاح طوله 8 كلمات ثنائية وحسب المعادلة الاتية :

Key = (array2 (Start)) XOR (Start Mod 255)

6. أضافة سطر في أسفل الصورة .

7. أعطاء السطر المضاف أسفل الصورة قيمة لونية متناسقة مع القيم اللونية للسطرين السابقين ومن ثم فأن القيم اللونية في السطر المضاف تصبح متناسقة مع القيم اللونية في الصورة .

8. أخفاء قيم وثوقية الصورة ووثوقية المستخدم (قيمة التوقيع الرقمي) في السطر المضاف باستخدام الرقم الثنائي الأقل أهمية ضمن كلمة ثنائية واحدة من كل نقطة

الشكل (2) يوضح خوارزمية تحقيق الوثوقية عند الجهة المرسلة .