الجمهورية العربيـة السـورية
المعهد العالي للعلوم التطبيقية والتكنولوجيا
قسـم الاتصالات
العام الدراسي 2016/2017

HIAST
Communication
Department

مشروع تخرج

أعدّ لنيل درجة الماجستير في الاتصالات

تعمية معطيات تلفزية باستخدام خوارزمية المسح SCAN وتنفيذها على بطاقة FPGA ومقارنتها مع خوارزمية التعمية المعيارية AES

تقديم

م.دريد جرماشي

إشراف

د. أميمة دكاك **د. داوود قره كوللّه**

30/10/2016

أهدي هذا العمل إلى أمي وأبي وزوجتي الغالية.

كلمة شكر

أتقدم بالشكر إلى كل من ساهم في إنجاز هذا العمل، وأخصّ بالشكر كلّاً من الدكتورة أميمة دكاك والدكتور داوود قره كوللّه، على مساعدتهما في هذا المشروع، وعلى ملاحظاتهما القيمة.

م.دريد جرماشي

الخلاصة

يهدف هذا المشروع إلى توصيف وتنفيذ تصميم عتادي لخوارزمية المسح باستخدام دارة قابلة للبرمجة FPGA، بحيث يستطيع هذا التصميم أن يمسح صور بدقة عالية في الزمن الحقيقي، على الرغم من أن خوارزمية المسح خوارزمية تعمية كتلية. جرى اختيار كتل بقياس 256x256 بيكسل لتأمين معدّل معطيات مناسب للعمل بالزمن الحقيقي. وقع الاختيار على تقنية FPGA لبناء الكيان الصلب لهذه الخوارزمية، لما تتمتع به من إمكانيات هائلة في الحجم والسرعة. في البداية، جرت دراسة وتوصيف هذه الخوارزمية باستخدام بيئة MATLAB، بهدف الحصول على نتائج مرجعية يمكن العودة إليها لمقارنة النتائج النهائية. ثم جرى تصميم الكيان الصلب للخوارزمية باستخدام لغة توصيف الكيان الصلب VHDL. أدّت المحاكاة في بيئة ModelSim إلى التأكد من صحة التصميم بالمقارنة مع النتائج المرجعية. جرت المقارنة بين أدائي خوارزمية المسح SCAN والخوارزمية المعيارية AES، وذلك بتطبيق العديد من اختبارات العشوائية، واختبار معاملات ترتبط بقوة خوارزمية التعمية، إضافة إلى مقارنة المجال المتاح لاختيار مفاتيح التعمية لكل منهما. ونتج عن هذه الاختبارات صلاحية خوارزمية التعمية "المسح SCAN" للاستخدامات الأمنية الشخصية والتجارية.

المحتويات

الخلاصة ..... **I**
المحتويات ..... **II**
قائمة الاشكال ..... **IV**
قائمة الجداول ..... **VI**
مسرد المصطلحات ..... **VII**
مقدمة عامة ..... **VIII**
الفصل الاول: لمحة تاريخية ونظرية للتعمية 1
1.1- مقدمة 2
2.1-لمحة تاريخية عن التعمية 2
3.1- الحاجة إلى التعمية في الحفاظ على أمن شبكة الإنترنت 3
4.1- تحديات الأمان 3
5.1- تحليل التعمية 4
6.1- أنواع التعمية 6
الفصل الثاني: محاكاة خوارزمية المسح SCAN ضمن بيئة MATLAB 9
1.2- مقدمة 10
2.2- التعمية باستخدام المسح 11
3.2- قواعد تشكيل مفاتيح التعمية (مخططات المسح المعممة) 14
4.2- تنفيذ محاكاة خوارزمية المسح 16
1.4.2- المخطط التدفقي للتعمية 16
2.4.2- المخطط التدفقي لفك التعمية 18
5.2- نتائج محاكاة الخوارزمية 19
الفصل الثالث: مقارنة أداء خوارزمية المسح SCAN مع أداء الخوارزمية المعيارية AES 22
1.3- مقدمة 32
2.3- لمحة عن خوارزمية التعمية المعيارية 23

3.3- مقارنة عدد المفاتيح المتاحة في كلا الخوارزميتين AES وSCAN 26
4.3- بعض الاختبارات المستخدمة لقياس أداء خوارزميات التعمية 27
5.3- التجارب والاختبارات 29
الفصل الرابع: بطاقة التطوير DE2-115 31
1.4- مقدمة 32
2.4- بطاقات FPGA 32
3.4- المنهجية العامة للتصميم باستخدام تقانة FPGA 33
4.4- البطاقة Altera DE2-115 34
5.4- الكاميرا الرقمية TRDB_D5M 38
الفصل الخامس: بناء الكيان الصلب لمعمّي ومفكّك تعمية المسح SCAN على شريحة FPGA 40
1.5- مقدمة 41
2.5- الأعمال ذات الصلة 41
3.5- المخطط التدفقي لخوارزمية المسح 42
4.5- التصميم الأول: تطبيق خوارزمية المسح على صورة بدقة 256×256 بيكسل 43
5.5- التصميم الثاني: تطبيق خوارزمية المسح على فيديو بدقة 256×256 بيكسل 45
6.5- الوحدات الأساسية المكوّنة للتصميمين 46
1.6.5- وحدة توليد العناوين Addresses Generator 46
2.6.5- وحدة تبديل قيم البيكسلات الخاصة بالتعمية Enc unit 51
3.6.5- وحدة تبديل قيم البيكسلات الخاصة بفك التعمية Enc unit 51
4.6.5- مولّد الأعداد العشوائية 52
الفصل السادس: اختبار أداء نظام الاتصال المعمّى باستخدام خوارزمية المسح SCAN 54
1.6- إختبار خوارزمية المسح SCAN 55
1.1.6- السيناريو الأول 55
2.1.6- السيناريو الثاني 56
3.1.6- السيناريو الثالث 56
4.1.6- السيناريو الرابع 57
2.6- الكلفة العتادية لكلّ من التصميمين 58
الفصل السابع: الخاتمة والآفاق المستقبلية 59

1.7- الأدوات المستخدمة في إنشاء نظام الإتصال المعمّى.....60
2.7- المشاكل والصعوبات 61
3.7- الخاتمة.....61
4.7- الآفاق المستقبلية 61
الملاحق 62
الملحق A: وحدة الإظهار VGA 63
المراجع.....66

قائمة الاشكال

الشكل 1.1– استخدام المفتاح السري في التعمية وفك التعمية في التعمية المتناظرة 7

الشكل 2.1– استخدام مفتاح في التعمية مختلف عن مفتاح فك التعمية في التعمية غير المتناظرة 8

الشكل 1.2– (a) مصفوفة ثنائية البعد 4x4(b) مخطط سن المنشار(c) يمثل مخطط مسح آخر.. 10

الشكل 2.2– مخططات التقسيم وتحويلاتها..... 11

الشكل 3.2– مخططات المسح الأولية..... 12

الشكل 4.2– مخطط المسح الأولي y مع تحويلاته الثمانية. 21

الشكل 5.2– (أ) مخططا مسح أوليان (ب) مخططا مسح موسّعان (ج) مخطط مسح معمّم..... 31

الشكل 6.2– الترميز الشجري لمخطط المسح المعمّم Scan_Key = X4 (i2 y3 Z5 (o1 a2 s5 b0)w1) 41

الشكل 7.2– الصورة الواضحة (يسار) والصورة المعمّاة (يمين) باستخدام المخطط scan_key. 41

الشكل 8.2– تمثيل مخطط المسح الأوليّ بالصيغة الثنائية..... 41

الشكل 9.2– تمثيل مخطط التقسيم بالصيغة الثنائية..... 51

الشكل 10.2– المخطط التدفقي لمحاكاة التعمية باستخدام خوارزمية المسح SCAN على MATLAB. 71

الشكل 11.2– المخطط التدفقي لمحاكاة فك تعمية خوارزمية المسح SCAN على MATLAB..... 19

الشكل 12.2– الواجهة الرئيسية لمحاكاة خوارزمية المسح..... 20

الشكل 13.2– (a) مخططات المسح الأولية في واجهة المستخدم، (b) مخططات التقسيم في الواجهة. 21

الشكل 14.2– مخطط المسح المعمّم (مفتاح التعمية) في واجهة المستخدم. 21

الشكل 1.3– مصفوفة التبديل S-box. 24

الشكل 2.3– الإزاحة الدورانية في خوارزمية التعمية المعيارية AES.. 24

الشكل 3.3– مصفوفة مزج الأعمدة..... 25

الشكل 4.3– الضرب بـ2 في الحقل GF(8)... 25

الشكل 5.3– الضرب بـ3 في الحقل GF(8)..... 25

الشكل 6.3– إضافة المفتاح الجزئي الموافق إلى مصفوفة 4×4 الناتجة من المرحلة السابقة.... 26

الشكل 1.4– العنصر المنطقي ومكوناته..... 33

الشكل 2.4– منهجية التصميم باستخدام FPGA. 34

الشكل 3.4– المخطط الصندوقي لبطاقات العائلة Cyclone IV E..... 35

الشكل 4.4– المبدل الرقمي التماثل VGA المضمّن في البطاقة DE2_115 35
الشكل 5.4– إشارة التزامن الأفقي..... 36
الشكل 6.4– شريحة EP4CE115F29 المضمنة فيي بطاقة DE2_115. 37
الشكل 7.4– ربط الكاميرا مع البطاقة بوصلة خارجية. 38
الشكل 8.4– توضع بيكسلات الألوان ضمن الأسطر. 38
الشكل 9.4– طريقة قراءة الصورة زمنياً..... 39
الشكل 10.4– استيفاء اللون الأخطر. 39
الشكل 1.5– المخطط التدفقي لنظام التعمية باستخدام خوارزمية المسح. 43
الشكل 2.5– المخطط الصندوقي للتصميم 44
الشكل 3.5– المخطط الزمني لتوليد العناوين.. 45
الشكل 4.5– المخطط الصندوقي للتصميم الثاني، الذي يقوم بتطبيق خوارزمية المسح SCAN على فيديو بدقة 256×256 بيكسل.. 46
الشكل 5.5– وحدة توليد العناوين Addresses Generator1. 47
الشكل 6.5– مثال عن مخطط تقسيم لصورة بقياس 256×256. 48
الشكل 7.5– مخطط ألة الحالة للمتحكم FSM. 50
الشكل 8.5– وحدة تبديل قيم البيكسلات في التعمية. 51
الشكل 9.5– وحدة تبديل قيم البيكسلات في فك التعمية. 52
الشكل 10.5– سجلات الإزاحة الخاصة ببعض بتات مولد الأعداد العشوائية. 53
الشكل 1.6– مثال عن مسح صورة بدون مرحلة إضافة القيم العشوائية. 55
الشكل 2.6– مثال عن تعمية صورة باستخدام خوارزمية المسح. 56
الشكل 3.6– لقطة للشاشة عند تعمية معطيات الكاميرا، بدون إضافة العشوائية..... 57
الشكل 4.6– لقطة للشاشة عند تعمية معطيات الكاميرا، مع إضافة العشوائية. 57
الشكل 1.7– العتاد الصلب المستخدم في نظام الاتصال المعمّى. 60
الشكل 1.A– مخطط دارة VGA..... 63
الشكل 2.A– مخطط VGA الصندوقي. 64
الشكل 3.A– التزامن الأفقي لنظام VGA. 64
الشكل 4.A– مواصفات التزامن العامودية لنظام VGA. 65

قائمة الجداول

الجدول 1.3– عدد المفاتيح الممكنة في خوارزمية المسح (يمين) وفي الخوارزمية AES (يمين). 27
الجدول 2.3– نتائج الاختبارات على كلّ من خوارزميتي التعمية: SCAN, AES. 30
الجدول 1.4– إشارات التزامن الأفقي. 36
الجدول 2.4– إشارات التزامن العمودي. 36
الجدول 1.6– الكلفة العتادية اللازمة لتنفيذ خوارزمية المسح SCAN. 58
الجدول 1.A– توصيف إشارات VGA. 64
الجدول 2.A– توصيف إشارات التزامن الأفقي في نظام VGA 65

مسرد للمصطلحات والاختصارات

SCAN: خوارزمية المسح لتعمية الصور والفيديو.

AES: خوارزمية معيارية متقدمة للتعمية (Advanced Encryption Standard).

Confusion: عملية أساسية في التعمية تسمى الخلط.

Diffusion: عملية أساسية في التعمية تسمى النثر.

Block: الكتلة هي مصفوفة مربعة، وتُعامل كعنصر.

Histogram: المخطط التكراري.

Cipher Key: مفتاح التعمية.

scan Key: مفتاح المسح هو مفتاح التعمية ويتميز بطوله المتغير.

Plain text: النص الواضح هو معطيات الدخل التي نريد تعميتها، ويمكن أن يكون صورة أو فيديو.

Cipher text: النص المعمّى هو خرج عملية التعمية، وهي بلا معنى إذا لم يتم فك تعميتها باستخدام مفتاح التعمية (تعمية متناظرة).

Ciphering: التعمية هي سلسلة من العمليات التي تحول النص الواضح إلى نص مُعمّى باستخدام مفتاح التعمية.

Deciphering (Inverse Ciphering): فك التعمية هي سلسلة من العمليات التي تحول النص المعمّى إلى نص واضح باستخدام مفتاح التعمية (في حالة التعمية المتناظرة).

Mean Square Error: الخطأ التربيعي الأصغري.

Structural Similarity Index Measure: معامل التشابه البنيوي.

Number of Changing Pixels Rate: نسبة عدد البيكسلات المتغيّرة.

Differential Attack: الهجوم التفاضلي.

Unified Averaged Changed Intensity: الكثافة المتوسطة الموحدة المتغيرة.

Jaccard Similarity: تشابه جاكارد.

Dynamic Time Warping: الانزياح الزمني الديناميكي.

Correlation: الترابط.

Plain text Sensitivity: حساسية للنص الواضح.

key Sensitivity: حساسية للمفتاح.

S-box: مصفوفة تبديل غير خطية، تُستخدم في تابع توسيع المفتاح في الخوارزمية المعيارية AES، لاستبدال قيمة البايتات، وهي تابع تقابل على البايتات (واحد لواحد).

مقدمة عامة

علم التعمية هو العلم المهتم بالتقنيات اللغوية والرياضية لتحقيق أمن المعلومات، المراد تخزينها أو نقلها. وقد اقتصر استخدام علم التعمية في القرون الماضية على الحفاظ على أمن المعلومات العسكرية، والمراسلات الدبلوماسية، وحماية الأمن الوطني. فقد ذُكِر أنَّ أوّل من قام بعمليّة التعمية للتراسل بين قطاعات الجيش هم الفراعنة، وكذلك كان للعرب محاولات في مجال التعمية، واستخدم الصينيون طرق عديدة في علم التعمية لنقل الرسائل أثناء الحروب. فقد كان قصدهم من استخدام التعمية إخفاء الشكل الحقيقي للرسائل، حتى لو سقطت في يد العدو، فإنه لن يستطيع فهمها. وأفضل طريقة استخدمت في التاريخ القديم هي طريقة القيصر جوليوس وهو أحد قياصرة الروم (طريقة إزاحة الأحرف). لكن نطاق تطبيقات التعمية توسع كثيراً في العصر الحديث بعد تطور الاتصالات، وارتبط العالم بعضه مع بعض عبر شبكات مفتوحة (شبكة الإنترنت). يجري استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين، أو بين المنظمات الخاصة والعامة، عسكرية كانت أم مدنية. وكان لابد من طرق تحفظ سرية المعلومات، وقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى، التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات. حيث أنّ نظم الاتصالات تتطلب نسباً متفاوتة الوثوقية بالإضافة إلى ضمان عدم الاختراق، منع التجسس والقرصنة الإلكترونية، وتأمين سبل التجارة الإلكترونية.

ينقسم علم التعمية إلى قسمين هما التعمية وكسر التعمية. حيث يكون هدف التعمية الأساسي هو ضمان سرية المعلومات المنقولة وعدم تعرضها للاعتداء من قبل محلّل التعمية (كاسر التعمية)، الذي يكون هدفه مضاداً تماماً للمُعمّي، وهو كسر التعمية، ومعرفة محتوى المعلومات المنقولة أو تحريفها بشكل يؤدي إلى قبولها على أنها المعلومات الصحيحة.

من هنا جاءت أهمية هذا المشروع الذي يهدف إلى تصميم أحد أهم خوارزميات التعمية المتخصصة بتعمية الصور والفيديو، وهي خوارزمية المسح SCAN.

تقدم معظم خوارزميات التعمية الحديثة أداءً جيداً من حيث قوة التعمية وانخفاض التعقيد، ولكن قلة من هذه الخوارزميات تختص بتعمية الصور والفيديو. حيث تقدم معظم الخوارزميات المطروحة جودة عالية من ناحية التعمية، لكن معدل منخفض من ناحية تدفق المعطيات.

تنتمي خوارزمية المسح SCAN إلى عائلة خوارزميات التعمية التكرارية المختصة بتعمية الصور والفيديو، حيث تقوم هذه الخوارزمية على عمليتين أساسيتين هما تبديل أماكن بيكسلات الصور وتغيير قيمة البيكسل الواحد.

تظهر قوة خوارزمية المسح من خلال عدد مفاتيح التعمية المتاحة، فيمكن أن يصل هذا العدد إلى رتبة 10^{29} مفتاحاً مختلفاً من أجل صورة صغيرة نسبياً مؤلفة من 8x8 بيكسل. أما في حالة صورة قياسها 16x16 بيكسل، فيمكن لهذا العدد أن يصل إلى رتبة 10^{117} مفتاحاً مختلفاً. حيث يزداد عدد مفاتيح التعمية المتاحة، أسياً مع زيادة أبعاد الصورة.

تُعنى خوارزمية المسح بكل من الضغط، الإخفاء والتعمية. لكننا في هذا البحث سوف نركز على التعمية فقط وذلك لتقليل التعقيد ولتحقيق إمكانية العمل في الزمن الحقيقي وبالتالي إمكانية تعمية الفيديو. أجرينا محاكاة لخوارزمية المسح ضمن بيئة MATLAB، من أجل تقييم التعقيد والأداء، بالإضافة إلى الحصول على نتائج مرجعية نستخدمها من أجل التصميم العتادي للخوارزمية على دارة FPGA. اخترنا إجراء المقارنات والتطبيقات العملية على صور بحجم 256x256 بيكسل، حيث يجري تمثيل كل بيكسل على 8-bits.

نعرض في الفصل الأول لمحة تاريخية ونظرية لعلم التعمية. نقدم في الفصل الثاني توصيفاً لخوارزمية المسح SCAN بالإضافة إلى محاكاة هذه الخوارزمية ضمن بيئة MATLAB. نعرض في الفصل الثالث أهم الاختبارات التي تقيس أداء خوارزميات التعمية ونقدم مقارنة بين خوارزمية المسح SCAN وخوارزمية التعمية المعيارية AES. نعرّف في الفصل الرابع بخواص وميزات بطاقة التطوير DE2_115 المستخدمة في المشروع. نعرض في الفصل الخامس المخطط العام للمشروع وخطوات بناء الكيان الصلب لخوارزمية المسح SCAN على شريحة FPGA. نعرض في الفصل السادس التجارب والاختبارات التي جرى تنفيذها، ونقدّم في الفصل الأخير الخاتمة والآفاق المستقبلية.

الفصل الأول

لمحة تاريخية ونظرية عن التعمية

يقدّم هذا الفصل لمحة تاريخية موجزة عن تطور التعمية، والفوائد التي تقدمها، وطرق إخفاء المعلومات السرية، بالإضافة إلى دراسة نظرية موجزة عن نظم التعمية.

1.1- مقدمة

يمكننا تعريف التعمية بأنها عملية حماية المعلومات القّيمة (المستندات، الصور، ....) لمنع الأشخاص غير المرخَّص لهم من الاطلاع على المعلومات أو فهمها أو تغييرها. تقوم عملية التعمية (خوارزمية التعمية) بتحويل النص الواضح (Plain Text) باستخدام مفتاح سري (Secret Key) إلى نص مُعمّى (Cipher Text).

ومن المعلوم أن الإنترنت تشكِّل في هذه الأيام الوسطَ الأضخم لنقل المعلومات. فمثلاً يتم نقل المعلومات الحساسة (مثل الحرَكات المالية) بصيغة مُعمّاة، للحفاظ على سلامتها وتأمينها من عبث المتطفلين والمخربين واللصوص. وتُستخدَم المفاتيح في تعمية (Encryption) الرسالة، وفك تعميتها (Decryption) . وتستند هذه المفاتيح إلى صِيَغ رياضية معقَّدة (خوارزميات). وتعتمد قوة وفعالية التعمية على عاملين أساسيين: الخوارزمية، وطول المفتاح مقدَّراً بالبتات (bits). ومن ناحية أخرى، فإن فك التعمية هو عملية استعادة البيانات بصيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك التعمية.

2.1- لمحة تاريخية عن التعمية

انتشرت التعمية قديماً منذ أكثر من 4000 سنة، وخاصةً في فترات الحروب حيث كان من الضروري نقل الأوامر العسكرية بسرية كاملة. وكانت تعتمد على طرق سرية لا يعلمها إلا مُستخدميها، وكانت تستخدم طرق مختلفة، تعتمد في أغلبها على تعمية النصوص. من هذه الطرق التبديل البسيط الذي يطبق تبديلاً على محارف اللغة، Playfair لتعمية الثنائيات المحرفية، Hill لتعمية الثلاثيات أو الرباعيات وطريقة التعمية المتعددة الأبجدية (Vigenere).

الجدير بالذكر أن التعمية تطورت وأصبحت المعطيات التي نود تعميتها على شكل صوت أو صورة أو نص أومعطيات حاسوبية عموماً، وأصبحت هذه المعطيات رقمية في غالب الأحيان (سلسلة من البتات) ومع ذلك بقيت تسمية النص الواضح للمعطيات الواضحة والنص المعمّى للمعطيات المعماة.

جرى طرح عدد قليل جداً من خوارزميات التعمية مخصصة للصور، ونادراً ما استخدم من أجل تعمية المعطيات الفيديوية، معظمها لا معقدة جداً ولا تحقق شروط العمل في الزمن الحقيقي. يوجد ثلاث أنواع مختلفة من الخوارزميات المخصصة لتعمية الفيديو:

- ⇦ **خوارزميات التعمية الكليّة:**

في هذا النوع يتم ضغط ملفات الفيديو ثم يتم تعميته، باستخدام إحدى خوارزميات التعمية التقليدية، مثل الخوارزمية المعيارية AES، خوارزمية IDEA أو خوارزمية DES. تعمي هذه الخوارزميات كتل من الصورة (الكتلة مكونة من 16-bytes في الخوازمية المعيارية AES)، ويتغير المفتاح بعد تعمية عدد من البيكسلات، وهي خوارزميات غير مناسبة للعمل في الزمن الحقيقي، وذلك بسبب تعقيد الخوارزمية الحسابي وسرعتها المنخفضة (خاصة من أجل الفيديوات عالية الدقة) [1].

⇦ **خوارزميات التبديل:**

يتميّز هذا النوع من خوارزميات التعمية بقلّة العمليات الحسابية اللازمة، واعتمادها بشكل أساسي على تبديل أماكن البيكسلات، يوجد العديد من الأمثلة على هذا النوع:

- خوارزمية تعمية الصورة الملوّنة بالإعتماد على خواص الصورة الواضحة (لمقاومة هجوم الصورة الواضحة المعروفة\المختارة) [2].
- خوارزمية تعمية الصورة بالإعتماد على تحويل أرنولد وعلى نظرية الفوضى، حيث تستخدم هذه الخوارزمية تحويل أرنولد لخلط الصورة (إخفاء الخواص التكرارية للصورة)، ثم تستخدم تقنية Tent mapping لتعمية الصورة الممزوجة [3].
- خوارزمية التبديل Zig-Zag التي تقوم بتقسيم كل إطار إلى كتل قياسها 8×8-PIXEL ووضعها في شعاع 1×64 وبترتيب مرتبط بالمفتاح السري للتعمية [13].
- خوارزمية التعمية المعتمدة على ترميز Huffman المستخدم في ضغط الفيديو MPEG. تقوم هذه الخوارزمية على استخدام ترميز مختلف (متقلق بمفتاح تعمية) لكن مشابه لترميز Huffman المعياري [14].

⇦ **خوارزميات التعمية الانتقائية:**

لا يقوم هذا النوع بتعمية كامل ملف الفيديو المضغوط، وإنما يجري اختيار أجزاء محددة فقط لتعميتها وهي بذلك لا تقدم مستوى أمان عالي. ومثال على هذا النوع الطريقة التي اقترحها Meyer and Gadegast، والتي تستخدم تعمية تقليدية مثل DES و AES لتعمية كل الترويسات والأطر المرجعية في ملفات الفيديو MPEG [15].

تنتمي الخوارزمية المعتمدة في مشروعنا وهي خوارزمية التعمية باستخدام مخططات المسح SCAN إلى النوع الثاني من خوارزميات تعمية المعطيات الفيديوية، والتي تعتمد على تبديل أماكن البيكسلات في كل إطار من إطارات الفيديو، وذلك بحسب مخطط المسح المعمّم (الذي يمثل مفتاح التعمية).

3.1- الحاجة إلى التعمية في الحفاظ على أمن شبكة الإنترنت

حملت شبكة الإنترنت التي تضم مجموعة كبيرة من الشبكات حول العالم فوائد جمّة، وأصبحت وسيلة سهلة وممتعة تُتيح لملايين البشر الولوجَ إلى كم هائل من المعلومات، إضافةً إلى التواصُل وتبادُل المعلومات والرسائل فيما بينهم. ولكن بعض العوامل (مثل الطبيعة المفتوحة لهذه الشبكة، وعدم وجود أي جهة يمكنها الادعاء بأنها تمتلكها أو تسيطر عليها، وعدم وجود قوانين مركزية رادعة)، أدَّت إلى انتشار العديد من الجرائم المرتكبة من جرّاء استخدام شبكة الأنترنت: كالتجسس على حُزم الرسائل الإلكترونية (Sniffing Packet)، تخريب أجهزة الكمبيوتر والوصول إلى الملفات السرية (Computer Hacking)، شَنّ هجوم الفيروسات على البريد الإلكتروني، إضافة إلى عمليات الخداع (Hoaxes). فأصبح أمن الإنترنت شأناً مهماً لا بد من حل مشاكله، نظرا لأهميته في عمليات تبادُل المعلومات الشخصية ومعلومات العمل. وتبقى عملية التعمية الرادع الوحيد المتاح للحفاظ على أمن المعلومات في شبكة اللإنترنت.

ولكي تُعتَبر خوارزميات التعمية آمنة عملياً، يجب ألا يتمكن أي شخص من كسرها والاطلاع على النص الواضح من خلال النص المعمّى، ضمن زمن التغطية وبالإمكانات الحاسوبية المتاحة عالمياً. حيث زمن التغطية هو الزمن الذي يجب أن نحافظ ضمنه على أمن وسرية المعلومة، وبعده تفقد المعلومة أهميتها. مثال ذلك نشر خبر طلعات جوية عسكرية ، زمن التغطية لهذه المعلومة هو ساعة، ويجب أن تبقى خلاله هذه المعلومة سرية وآمنة، أما بعد ساعة وبعد تحليق الطائرات في الجو، تصبح هذه المعلومة بدون أي قيمة.

4.1- تحديات الأمان

توفر الخوارزميات المختلفة درجات أمان مختلفة، ويعتمد ذلك على مدى الصعوبة في كسرها. فإذا كانت تكلفة كسر الخوارزمية أعلى من قيمة المعلومات المعمَّاة بها، كانت الخوارزمية آمنة. وإذا كان الزمن اللازم لكسر الخوارزمية أطول من الزمن الذي يجب أن تبقى فيه المعلومات المعمَّاة سرية، كانت الخوارزمية آمنة. علماً أنّ الاحتمالات قائمة لفتوح جديدة في تحليل التعمية. وتكون خوارزمية التعمية آمنة دون شروط إذا لم تكن هناك معلومات كافية لاستعادة النص الواضح، مهما تكن كمية النص المعمَّى المتاحة للمحلّل. في الحقيقة، معمي دفتر المرة الواحدة One-Time Pad (وهو مُعمّي يستخدم مفتاح التعمية لمرة واحدة، ويغيّر المفتاح كُلما غيّر النص الواضح.) هو المعمِّي الوحيد غير القابل للكسر، حتى بتوفر إمكانات لا نهائية. أما نظم التعمية الأخرى، فجميعها قابلة للكسر بتوفر الوقت الكافي، حيث يمكن كسرها بالهجوم بالنص المعمَّى فقط، وذلك بتجربة كل المفاتيح الممكنة، واحد تلو الآخر، والتأكد من أن النص الواضح الناتج له معنى. يُسمى هذا الهجوم بالهجوم بالبحث الشامل Brute Force Attack.

يتلخص هدف جميع مستخدمي الإنترنت في الحصول على المعلومات ونقلها بشكل آمن، وهناك مجموعة من التحديات التي يجب أخذها في الحسبان لضمان نقلٍ آمن للمعلومات بين الأطراف المتصلة، وتنحصر هذه التحديات في ثلاثة محاور هي:

الخصوصية (Privacy)، وسلامة المعلومات (Integrity)، والتحقق من هوية الأطراف الأخرى (Peer Authentication) [4].

- خصوصية المعلومات (Privacy): كي تتم المحافظة على خصوصية المعلومات الإلكترونية، يجب ألا يتمكَّن من الاطلاع عليها إلا الأطراف المسموح لها بذلك. وللحفاظ على الخصوصية، لا بُدَّ من التحكم بعملية الولوج، وأكثر طرق التحكم انتشاراً هي: استخدام كلمات المرور (Passwords)، والجدار الناري (Firewall)، إضافة إلى شهادات الترخيص (Certificates Authorization). وهنا تجدُر الإشارة إلى أمر بالغ الأهمية؛ وهو أن على المستخدِم الحفاظ على سرية كلمة المرور، لأنها تشكل خط الدفاع الأول في وجه الولوج غير المرخَّص. وبهذه الطرق، يُمكن منع حدوث الجرائم المتعلقة بانتهاك الخصوصية مثل: التنصُّت (Eavesdropping)، واستعراض معلومات معيَّنة بدون ترخيص.
- سلامة المعلومات (Integrity): لا بُدَّ من حماية عمليتي نقل المعلومات وتخزينها، وذلك لمنع أي تغيير للمحتوى بشكل متعمَّد أو غير مُتعمَّد. وتكمن أهمية ذلك في الحفاظ على محتوى مفيد وموثوق به. وفي الغالب، تكون الأخطاء البشرية وعمليات العبث المقصود هي السبب في تلف أو تشويه البيانات. وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام. ولتلافي تشويه أو تلف البيانات، يُمكن استخدام تقنيات مثل: البصمة الإلكترونية للرسالة (Digest Message) والتعمية (Encryption)، ومن المفيد أيضاً استخدام برمجيات مضادة للفيروسات (Software Anti-Virus) لحماية أجهزة التخزين من انتهاكات الفيروسات التي تتسبب في تلف أو تشويه البيانات. ومن المهم أيضاً الاحتفاظ بِنُسَخ احتياطية (Backup) لاسترداد البيانات المفقودة في حال تعرضها للضرر، أو في حال تعطُّل الشبكة أثناء عملية النقل.
- التحقق من هوية الأطراف الأخرى (Peer Authentication): يجب التأكد من هوية الأطراف المعنية بعملية تبادل البيانات، إذ يجب على كلا الطرفين معرفة هوية الآخر لتجنب أي شكل من أشكال الخداع (مثل عمليات التزوير وانتحال الشخصيات). وهناك بعض الحلول والإجراءات للتحقق من هوية الأطراف المتصلة مثل: كلمات المرور (Passwords)، والتواقيع الرقمية (Digital Signatures)، والشهادات الرقمية (Digital Certificates) التي يُصدرها طرف ثالث. ويُمكن أيضا تعزيز الأمن بالاعتماد على بعض المميزات المحسوسة مثل: بصمة الإصبع (Print Finger)، والصوت، إضافة إلى الصورة.

5.1- تحليل التعمية

الغرض الأساسي من التعمية هو الحفاظ على سرية الرسالة (النص الواضح)، وعدم تمكن المتجسس (والذي يسمى أيضاً الخصم، أو المهاجم، أو المتطفل، أو الدخيل أو العدو) من معرفة مضمون الرسالة، على الرغم من قدرته على النفاذ إلى الاتصالات بين المرسل والمستقبل.

أما تحليل التعمية فهو علم الحصول على النص الواضح للرسالة المعماة دون معرفة المفتاح، وهو البحث عن نقطة ضعف في نظام التعمية يؤدي إلى معرفة النص الواضح أو المفتاح.

ويسمى تحليل التعمية عادة هجوماً Attack، ويُفترض عادةً أن مُحلِّلي التعمية يعرفون تفاصيل كاملة عن خوارزمية التعمية وطريقة تنفيذها. رغم أن المحلِّلين الحقيقيين لا يملكون كل هذه التفاصيل بشكل كامل، ولكن مع ذلك الأخذ بهذه الفرضية يُجنب الوقوع بالكثير من الأخطاء.

يوجد عدة أنواع عامة من الهجوم على نظم التعمية، وذلك حسب المعرفة التي يملكها محلِّل التعمية المهاجم[4] :

1. هجوم النص المعمّى فقط ciphertext-only attack:

   يمتلك محلِّل التعمية النصوص المعماة لعدة رسائل عُمِّيت باستخدام نفس خوارزمية التعمية. ومهمته هي الاستعانة بهذه النصوص واستعادة النص الواضح لأكبر عدد ممكن من الرسائل، والأفضل هو الحصول على مفتاح التعمية المستخدم في تعميتها ليتمكن من فك تعمية رسائل أخرى معمَّاة بالمفتاح نفسه، أو استنتاج خوارزمية لاستنتاج النص الواضح من معرفة النص المعمّى دون الحاجة لاستخدام المفتاح.

2. هجوم النص الواضح المعلوم known-plaintext attack:

   يمتلك محلِّل التعمية نصوصاً مُعمّاة لعدة رسائل، بالإضافة إلى النصوص الواضحة لهذه الرسائل. ومهمته هي الحصول على مفتاح التعمية المستخدم في تعميتها ليتمكن من فك تعمية رسائل أخرى معمَّاة بالمفتاح نفسه، أو استنتاج خوارزمية لاستنتاج النص الواضح من معرفة النص المعمّى دون الحاجة لاستخدام المفتاح.

3. هجوم النص الواضح المختار chosen-plaintext attack:

   يمتلك محلِّل التعمية نصوصاً مُعمّاة والنصوص الواضحة الموافقة لعدة رسائل، إضافة إلى أنه يستطيع اختيار النص الواضح الذي تجري تعميته باستخدام المفتاح. ومهمته هي الحصول على مفتاح التعمية المستخدم في تعميتها ليتمكن من فك تعمية رسائل أخرى معمَّاة بالمفتاح نفسه، أو استنتاج خوارزمية لاستنتاج النص الواضح من معرفة النص المعمّى دون الحاجة لاستخدام المفتاح. وهذا الهجوم أقوى من الهجوم بالنص الواضح المعلوم.

4. هجوم النص الواضح المختار المتكيِّف adaptive-chosen-plaintext attack:

وهو حالة خاصة من هجوم النص الواضح المختار، حيث يستطيع المحلِّل اختيار النص الواضح الذي تجري تعميته، إضافة إلى امكانية تعديل اختياره بناءً على نتائج التعمية السابقة. حيث يُفضَّل في حالة الهجوم بالنص الواضح المختار اختيار نص واضح كبير نسبياً لتعميته، بينما هنا في هجوم النص الواضح المختار المتكيِّف يمكن اختيار نص واضح أصغر لتعميته، ثم يمكن اختيار نصوص أخرى اعتماداً على النتيجة الأولى، وهكذا بالتتابع.

5. هجوم النص المعمَّى المختار chosen-ciphertext attack:

يمتلك محلِّل التعمية إمكانية اختيار نصوص مُعماة مختلفة لفك تعميتها، ولديه معرفة بالنصوص الواضحة المقابلة لكل منها. مثلاً لدى المحلِّل صندوق مُغلق يقوم بفك التعمية آلياً. ومهمته هي الحصول على مفتاح التعمية. يُسمى أحياناً الهجوم بالنص الواضح المختار والهجوم بالنص المعمَّى المختار معاً بالهجوم بالنص المختار.

6. الهجوم بالمفتاح المختار chosesn-key attack:

إن هذا الهجوم لايعني أن مُحلِّل التعمية يستطيع اختيار مفتاح التعمية، بل يعني انه يملك بعض المعرفة عن العلاقة بين المفاتيح المختلفة. وهذا الهجوم غريب وغامض وغير عملي.

7. تحليل التعمية باستخدام السوط:

يقوم المحلِّل بتهديد جهة ما أو ابتزازها أو تعذيبها حتى تعطيه المفتاح. وتُعرف الرشوة بالهجوم بشراء المفتاح. تعد هذه الطرائق هجوماً فعالاً، وغالباً ما تكون السبيل الأفضل لكسر الخوارزميات.

6.1- أنواع التعمية

يوجد نوعان مختلفان للتعمية هما [4]:

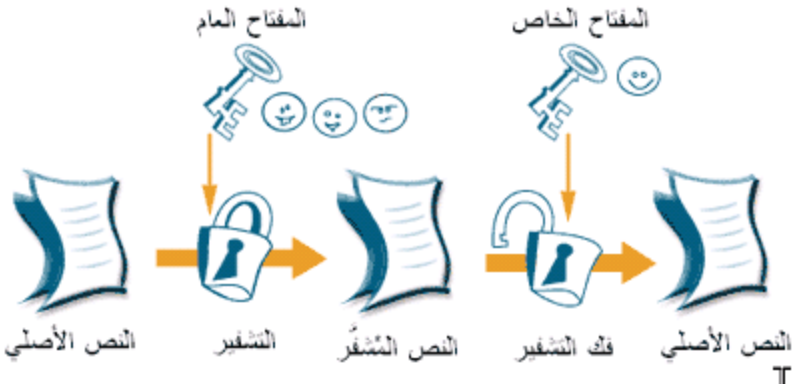
- التعمية المتناظرة (وتُسمى أيضاً بالمفتاح السري): في التعمية المتناظرة يستخدم كل من المرسِل والمستقبِل المفتاحَ السري ذاته، في تعمية (تشفير) الرسالة وفك تعميتها (فك تشفيرها). ويتفق الطرفان في البداية على المفتاح السري (Secret Key) التي سيتم استخدامه، حيث يستخدمه المرسِل لتحويل النص الواضح (Plain Text) إلى نص مُعمّى (Cipher Text)، ويستخدمه المستقبِل من أجل فك تعمية النص المعمّى (cipher text or encrypted text) واستنتاج النص الأصلي المفهوم. من ميزاته صغر حجم المفتاح وسرعة التعمية وفك التعمية، ولكن في هذا النوع من التعمية توجد ثغرة كبيرة، تكمن في تبادُل المفتاح السري في بيئة غير آمنة. والشكل (1.1) يمثل التعمية المتناظرة.

الشكل (1.1) استخدام المفتاح السري في التعمية وفك التعمية في التعمية المتناظرة.

تنقسم التعمية المتناظرة إلى نوعين تبعاً لتدفق المعطيات التي يتم تعميتها وفك تعميتها: التعمية الكتلية والتعمية الدفقية.

- التعمية الكتلية (Block Cipher): تُقسَّم النصوص الواضحة إلى كتل من البتات المتساوية الطول، طول الكتلة بين 32 و256 بت، وتُنفَّذ خوارزمية التعمية على الكتل، من أهم خوارزميات التعمية الكتلية: AES وDES وIDEA.
- التعمية الدفقية (Stream Cipher): هنا تُنفّذ التعمية على كتل بطول 1 (بت واحد أو بايت واحد)، ومن الأمثلة على هذا النوع من التعمية خوارزمية RC4 المستخدمة في SSL وفي WiFi، وخوارزمية E0/1 المستخدمة في Bluetooth، والخوارزميات A5/1,A5/2,A5/3 المستخدمة في GSM.

- التعمية غير المتناظرة (أو تعمية المفتاح العام): جاءت التعمية غير المتناظرة حلاً لمشكلة التبادل غير الآمن للمفاتيح في الوصلات غير الآمنة عند استعمال التعمية المتناظرة. عوضاً عن استخدام مفتاح واحد، تَستخدِم التعمية غير المتناظرة مفتاحين تربط بينهما علاقة. ويُسمى هذان المفتاحان المفتاح العام (Public Key)، والمفتاح الخاص (Private Key). يستخدم الأول لتعمية الرسالة، و يستخدم الثاني لفك تعمية الرسالة. حيث يتم تبادل المفتاح العام الذي يُستخدَم لتعمية الرسالة من جهة المرسل. أما المفتاح الخاص فلا يتم تبادله يُستخدم لفك تعمية الرسالة من جهة المستقبل. من ميزات هذا النوع هو إمكانية تبادل المفاتيح في بيئة غير آمنة، ولكنّ خوارزمياته بطيئة. الشكل (2.1) يمثل التعمية غير المتناظرة.

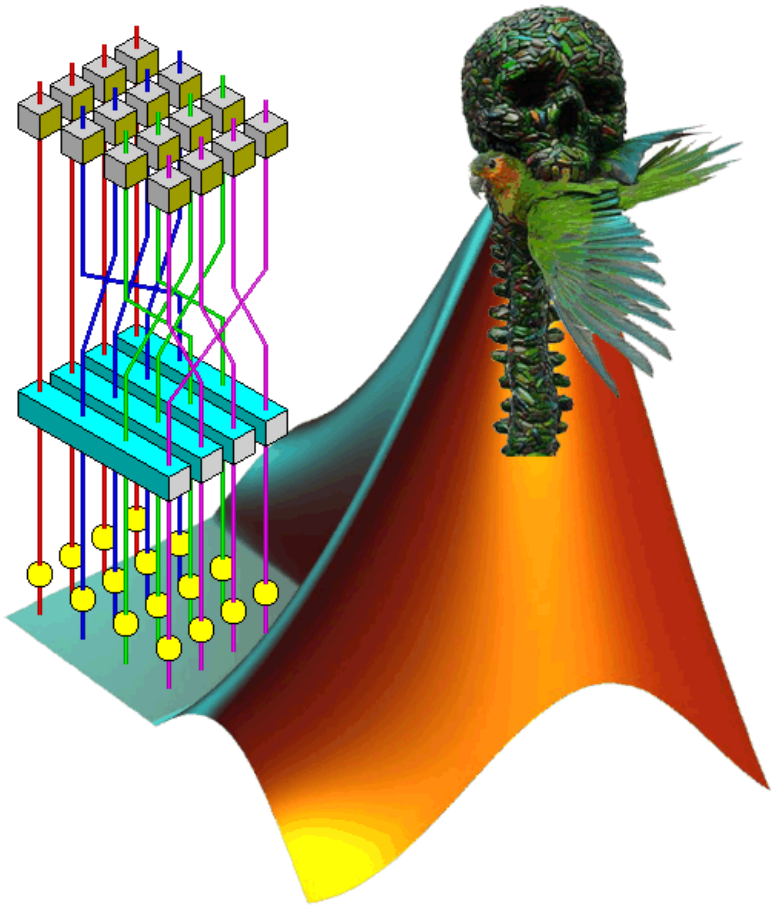


الشكل (2.1) استخدام مفتاح في التعمية مختلف عن مفتاح فك التعمية في التعمية غير المتناظرة.

وقع الاختيار في هذا المشروع على دراسة خوارزمية التعمية المتناظرة الكتلية باستخدام مخططات المسح SCAN، وإمكانية تنفيذيها على بطاقة FPGA.

الفصل الثاني

توصيف خوارزمية المسح SCAN ومحاكاتها ضمن بيئة MATLAB

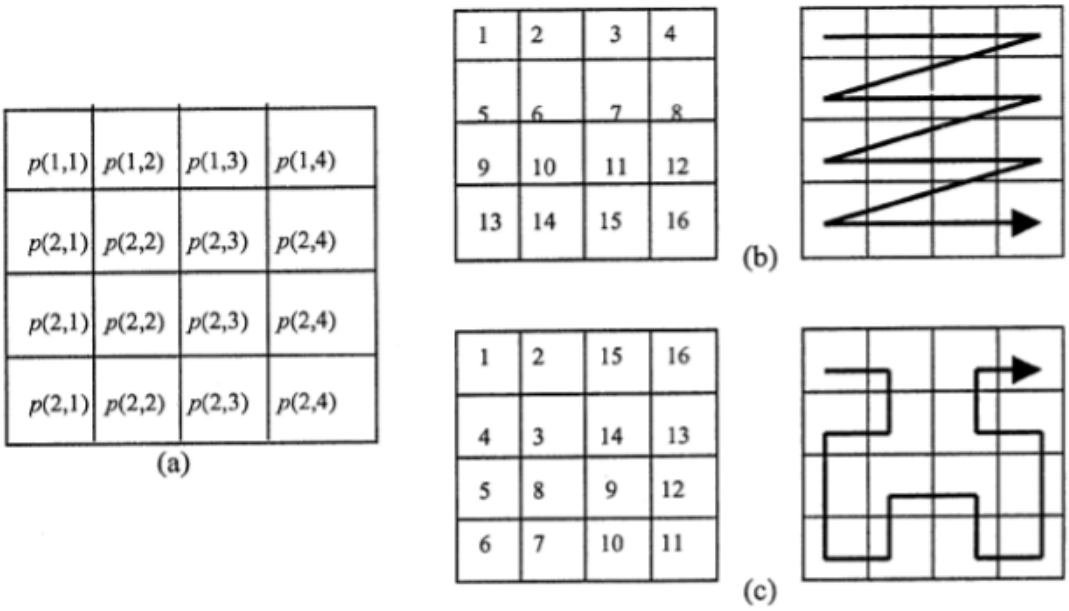


في بداية المشروع لا بدَّ من توصيف خوارزمية المسح SCAN ومن ثمّ إجراء محاكاة لعملها، وذلك لمقارنة النتائج التي سنحصل عليها فيما بعد، عند تنفيذ الخوارزمية على بطاقة FPGA. نقدّم في هذا الفصل تعريفاً لخوارزمية المسح بالإضافة إلى استعراض محاكاة الخوارزمية ضمن بيئة MATLAB.

1.2- مقدمة

يُعرّف مسح مصفوفة ثنائية البعد بأنه الوصول إلى كل عنصر من عناصر هذه المصفوفة مرة واحدة فقط، وبالتالي تتم معالجة عنصر من هذه المصفوفة مرة واحدة فقط خلال عملية المسح [5]. نعلم أنه في حالة مصفوفة NxN ثنائية البعد، يوجد !(N×N) نمط مسح مختلف، وكمثال على ذلك يوجد للمصفوفة الثنائية البعد المكونة من 4x4 عنصر، أنماط مسح عددها (10^{13} ~ 20,922,789,888,000 = !16 = !(4*4)). يُظهر الشكل (1.2) مثالاً عن نمطين من أنماط المسح للمصفوفة ثنائية البعد 4x4، أحدهما هو مخطط سن المنشار raster، المعروف والمنتشر بشكل واسع (المستخدم لمسح شاشة التلفاز أو الحاسوب).

خوارزمية المسح SCAN هي خوارزمية كتلية (block) متناظرة (symmetric)، يمكن أن يكون طول مفتاحها السري متغير، وذلك حسب حجم الصور المعماة، وحسب عمق التقسيمات التي نستخدمها. ويجري التعامل مع الكتل بشكل مصفوفات مربعة من البيكسلات بحجم 256×256 بيكسل، ويجري تمثيل البيكسل الواحد على بايت واحد أي على 8-bit. تعتمد خوارزمية المسح المقدمة في هذا المشروع، بشكل أساسي، على إعادة ترتيب بيكسلات الصورة، وتتم عملية إعادة الترتيب عن طريق استخدام نمط مسح، يمثل هذا النمط مفتاح التعمية وفك التعمية بآن واحد (تعمية بمفتاح متناظر)، سنقدّم فيما يلي دراسة عن هذه الخوارزمية.



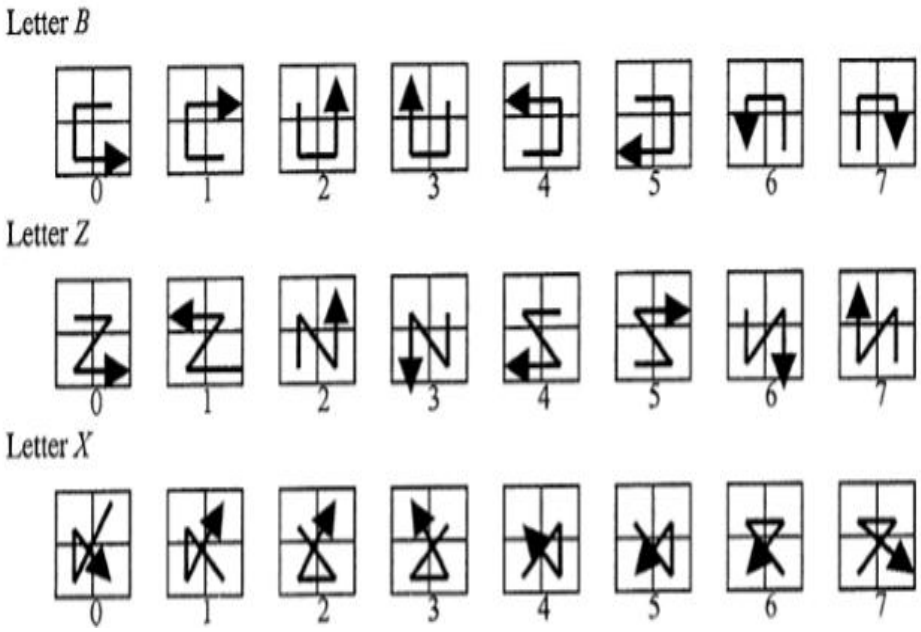
الشكل (1.2): (a) مصفوفة ثنائية البعد 4x4. (b) مخطط مسح بسن المنشار. (c) مخطط مسح آخر.

2.2- التعمية باستخدام المسح

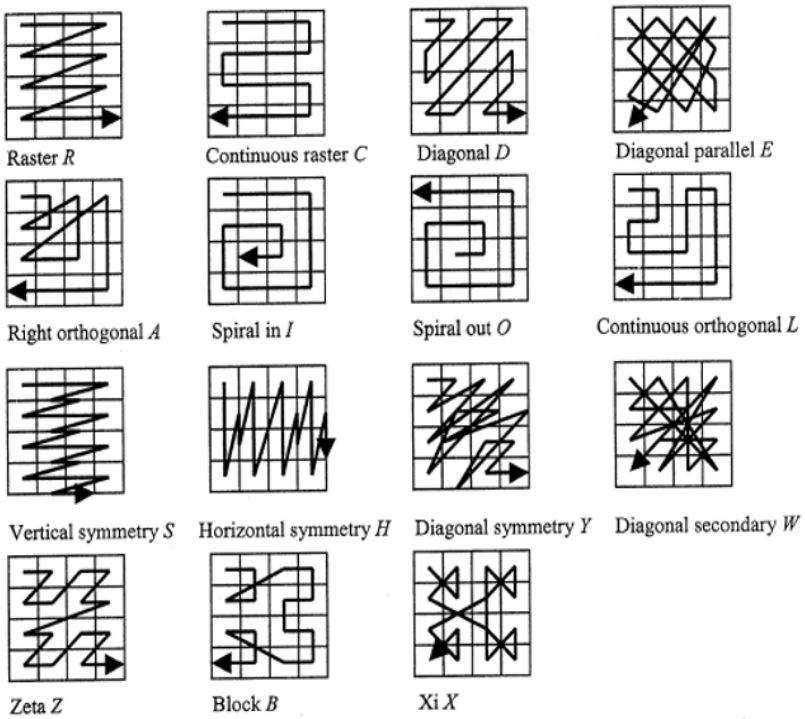
يمكن التعامل مع المسح على أنه منهج لغة، يمكن من خلال استخدام القواعد الخاصة لهذه اللغة؛ خلق عدد كبير جداً من مخططات المسح المختلفة لمصفوفة ثنائية البعد. يوجد منهجيات مسح مختلفة عن بعضها تعتمد على التطبيقات المختلفة، مثل المسح البسيط (simple SCAN)، والمسح الموسّع (extended SCAN)، والمسح المعمّم (generalized SCAN)، وتملك كلّ من هذه المنهجيات مجموعة مختلفة من مخططات المسح.

تُعرّف خوارزمية المسح على أنها لغة مترابطة لا تعتمد على السياق، مهمتها الوصول بشكل تتابعي إلى عناصر مصفوفة ثنائية البعد، وذلك بتوليد طيف واسع من مخططات المسح [5]. وتتألف أبجدية هذه اللغة، كما هو مبين في الشكلين (2.2) وَ (3.2)، من:

- ثلاثة مخططات تقسيم: B, X, Z.
- خمسة عشر مخطط مسح أوليّ: a, b, c, d, e, h, i, l, o, r, s, w, x, y, z.



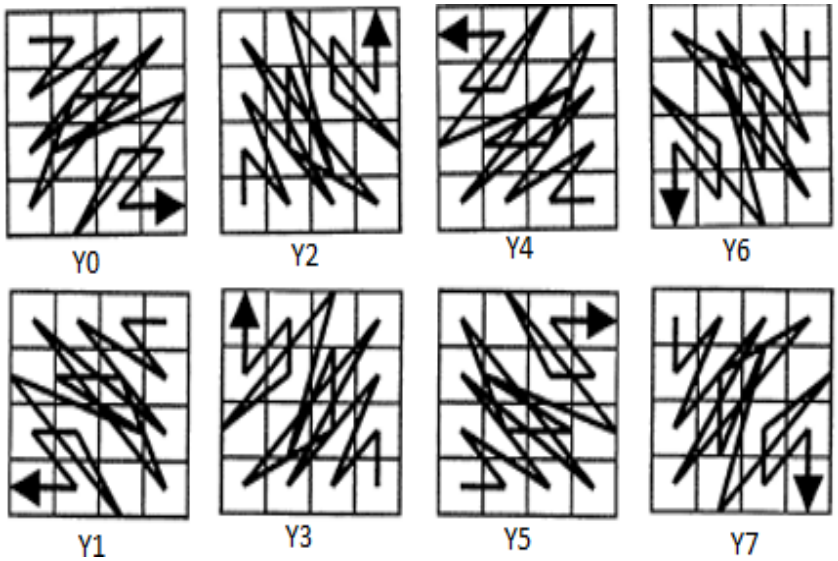
الشكل (2.2) مخططات التقسيم وتحويلاتها.



الشكل (3.2) مخططات المسح الأولية.

يرتبط كل مخطط (تقسيم أو مسح) بثمانية تحويلات مختلفة، يجري ترقيمها من 0 إلى 7. يظهر في الشكل (4.2) أحد مخططات المسح الأولية والتحويلات الثمانية الموافقة له.

يقوم مخطط التقسيم بتجزئة الصورة إلى أربع صور جزئية، يجري مسحها وفق ترتيب معين، بينما يجري مسح كل صورة جزئية وفقاً لمخطط مسح أولي خاص بها.



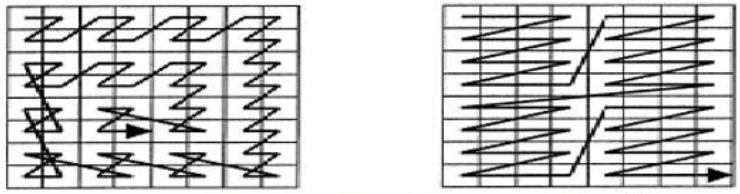
الشكل (4.2) مخطط المسح الأولي y مع تحويلاته الثمانية.

تقوم الفكرة الأساسية لتعمية الصورة باستخدام خوارزمية المسح، على إعادة ترتيب بيكسلات الصورة، وتغيير قيمة كل بيكسل، وذلك من خلال إضافة قيم عشوائية لها. يجري إعادة الترتيب باستخدام مجموعة من مخططات التقسيم والمسح. ويتم تغيير قيمة البيكسل باستخدام إجرائية تبديل بسيطة، بحيث تضيف قيماً عشوائية جرى توليدها باستخدام سجلات إزاحة بتغذية خلفية خطية، بحيث تضيف هذه الإجرائية خاصتي الخلط Confusion والنثر Diffusion إلى الصورة المعمّاة. تتلخص مهمتا الخلط والنثر في جعل مخطط التكرارات Histogram للصورة المعمّاة مسطحاً، وهذا بدوره يمنع كسر التعمية باستخدام المخطط التكراري. يجري تطبيق عمليتي إعادة الترتيب وتبديل القيم بشكل متداخل ومتكرر، وذلك لزيادة أثر الخاصتين السابقتين. يمثل الشكل (5.2) أمثلة عن مخططات مسح بسيطة وموسّعة ومعممّة.

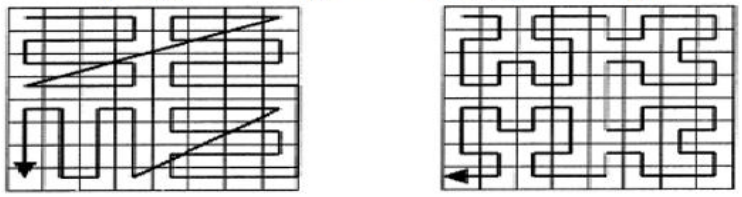
لنأخذ مخطط المسح المعمّم في المثال التالي:

scan_key = X4 (i2 y3 Z5 (o1 a2 s5 b0) w1)

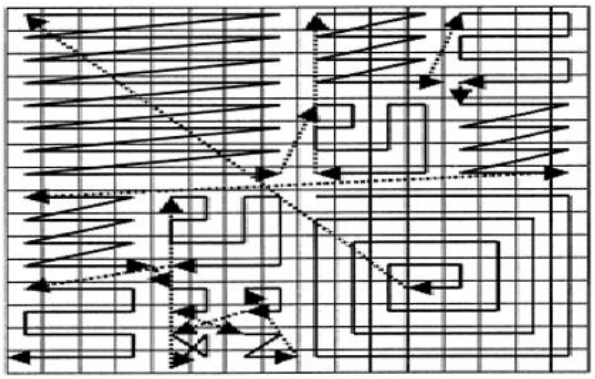
يتألف مخطط المسح المعمّم scan_key من مخططي تقسيم وعدد من مخططات المسح الأولية. في البداية، يقسم مخطط التقسيم X_4 الصورة إلى ثلاثة مخططات مسح أولية: i_2, y_3, w_1، بالإضافة إلى مخطط التقسيم Z_5 الذي يقوم بدوره بتقسيم الجزء الثالث من الصورة إلى أربعة مخططات مسح أولية: o_1, a_2, s_5, b_0. يمثل دليل المخطط رقم التحويل المطبق على المخطط. يبين الشكل (6.2) الترميز الشجري لمخطط المسح المعمّم في المثال السابق، كما يبين الشكل (7.2) خرج خوارزمية المسح بعد تطبيقها على صورة رمادية.



(أ) مخطط مسح بسيط (مخطط تقسيم + مخطط مسح واحد)

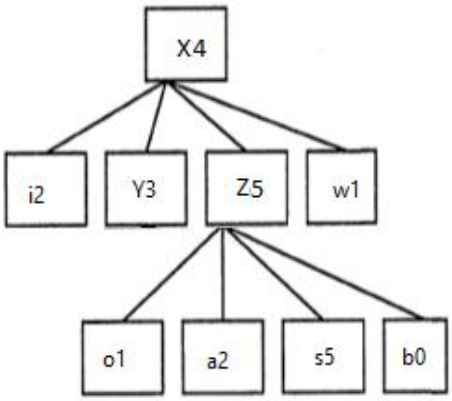


(ب) مخطط مسح موسع (مخطط تقسيم + عدة مخططات مسح)

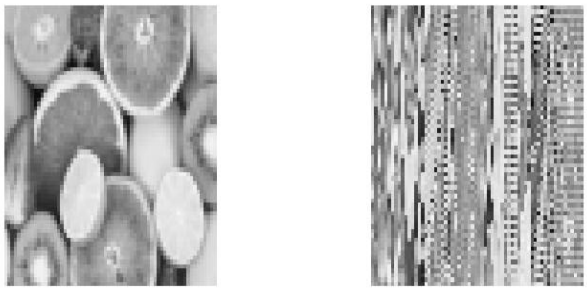


(ج) مخطط مسح معمّم (عدة مخططات تقسيم + عدة مخططات مسح)

الشكل (5.2): (أ) مخططا مسح بسيطان، (ب) مخططا مسح موسّعان، بينما (ج) مخطط مسح معمّم.



الشكل (6.2) الترميز الشجري لمخطط المسح المعمّم $scan_key = X_4 (i_2\, y_3\, Z_5 (o_1\, a_2\, s_5\, b_0) w_1)$

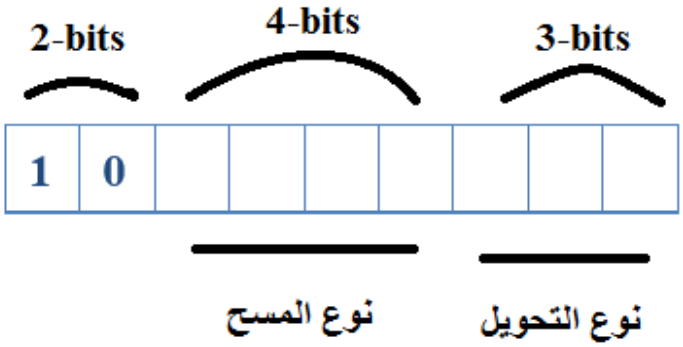


الشكل (7.2) الصورة الواضحة (إلى اليسار) والصورة المعمّاة (إلى اليمين) باستخدام مخطط المسح المعمّم scan_key.

3.2- قواعد تشكيل مفاتيح التعمية (مخططات المسح المعممة)

يتألف مخطط المسح المعم المعمّم م من تتالي مخططات تقسيم ومسح، يمكن تمثيلها بالصيغة الثنائية على الشكل التالي:

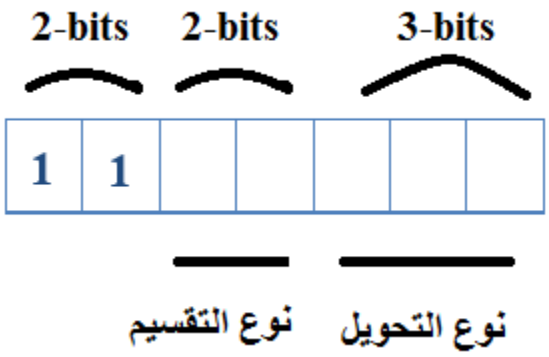
- يجري تمثيل مخطط المسح الأوليّ على 9-bits، كما هو مبيّن في الشكل (8.2).



الشكل (8.2) تمثيل مخطط المسح الأوليّ بالصيغة الثنائية.

- يُستخدم أول بيتين لتحديد نوع المخطط. يجري تمثيل نوع المخطط على 2-bits، يأخذان في حالة مخطط المسح الأوليّ القيمة '10'.
- تُستخدم البتات الأربعة التالية لتحديد نوع المسح الأولي. يوجد خمسة عشر مخطط مسح أوليّ، يجري تمثيلها على 4-bits.
- تُستخدم آخر ثلاث بتات لتحديد رقم التحويل المطبق على مخطط المسح الأولي. يوجد ثماني تحويلات مطبقة على كل مخطط، يجري تمثيلها على 3-bits.

- يجري تمثيل مخطط التقسيم على 7-bits، كما هو مبيّن في الشكل (9.2).



الشكل (9.2) تمثيل مخطط التقسيم بالصيغة الثنائية.

- يُستخدم أول بيتين لتحديد نوع المخطط. يجري تمثيل نوع المخطط على 2-bits، يأخذان في حالة مخطط التقسيم القيمة '11'.
- يُستخدم البتان التاليان لتحديد نوع التقسيم. يوجد ثلاثة مخططات تقسيم، يجري تمثيلها على 2-bits.
- تُستخدم آخر ثلاث بتات لتحديد رقم التحويل المطبق على مخطط التقسيم. يوجد ثماني تحويلات مطبقة على كل مخطط مسح، يجري تمثيلها على 3-bits.

- يجري تمثيل نهاية المفتاح بالبت '0'.

يجري تمثيل مفتاح التعمية $scan_key = X_4\,(i_2\, y_3\, Z_5\,(o_1\, a_2\, s_5\, b_0) w_1)$ الموجود في المثال السابق وفق الخطوات التالية:

- يجري تمثيل مخطط التقسيم X_4 بسلسلة البتات '11110100'، حيث يجري قراءة البتات من اليسار إلى اليمين كما يلي: يعبر البتان '11' عن أنّ نوع المخطط مخطط تقسيم، ويعبر البتان '10' عن مخطط التقسيم X، وتمثل البتات الثلاثة الأخيرة '100' رقم التحويل وهو هنا 4.
- يجري تمثيل مخطط المسح الأولي i_2 بسلسلة البتات '100101010'، وذلك كما يلي: يعبر البتان '10' عن أنّ نوع المخطط هو مخطط مسح أولي، وتمثل البتات الأربعة '0101' مخطط المسح الأولي i، وتمثل البتات الثلاثة الأخيرة '010' رقم التحويل وهو هنا 2.
- وبالمثل من أجل بقية المخططات:

'101010011'	y_3
'1101101'	Z_5
'100110001'	o_1
'100100010'	a_2
'101000101'	s_5
'101101000'	b_0
'101011001'	w_1

- ويجري تمثيل نهاية المفتاح بالبت '0'.

وبالتالي يجري تمثيل مفتاح التعمية scan_key بسلسلة البتات التالية:

scan_key= "111110100 100101010 101010011 1101101 100110001 100100010 101000101 101101000 101011001 0"

4.2- تنفيذ محاكاة خوارزمية المسح

جرت محاكاة خوارزمية المسح باستخدام بيئة MATLAB لكل من عمليتي التعمية وفك التعمية. وذلك وفق المخطط التدفقي للتعمية ولفك التعمية الموضّح في الشكلين (10.2) و(11.2) على الترتيب.

1.4.2- المخطط التدفقي للتعمية

يتألف المخطط التدفقي لعملية محاكاة جزء التعمية باستخدام خوارزمية المسح من الأجزاء التالية:

أ- وحدة تحصيل الصورة:

نعتبر أنّ الكتل هي صور قياسها 256×256 بيكسل، حيث يجري تطبيق مفاتيح التعمية على هذه الكتل. تُعتبر هذه الكتل مناسبة لتطبيقات الزمن الحقيقي (تطبيقات الفيديو وغيرها)، ومناسبة من حيث الأمان، حيث يكون عدد المفاتيح المتاحة من أجل هذه الكتل كبير جداً. يجري في هذه الوحدة قراءة الصورة الواضحة.

ب–وحدة قراءة مفتاح التعمية:

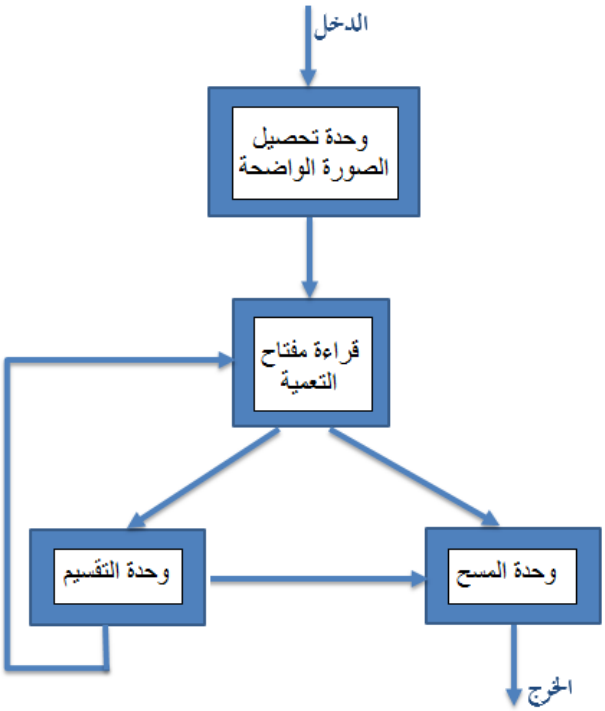
عند تنفيذ عملية تعمية الكتلة يجري قراءة المفتاح بشكل موازٍ، وذلك حسب قواعد تشكيل المفتاح. ويجري معرفة المخطط الحالي واتخاذ القرار فيما إذا كان مخطط مسح أوليّاً أو مخطط تقسيم، وتحديد نوع المخطط (يوجد خمسة عشر مخطط مسح أولي، وثلاثة مخططات تقسيم)، والتحويل المطبق عليه، وتمرير هذه المعاملات إلى الوحدة التالية، التي هي وحدة المسح أو وحدة التقسيم.

ت–وحدة المسح:

تقوم هذه الوحدة بتعمية الصورة الواضحة بقياس 256×256 بيكسل أو أي جزء منها، وتحويله إلى صورة مُعمّاة. دخل هذه الكتلة هو الصورة الواضحة بالإضافة إلى نوع مخطط المسح الأولي ورقم التحويل المطبق عليه، ولها خرج وحيد هو مصفوفة الصورة المعمّاة، التي لها نفس حجم صورة الدخل الواضحة.

ث–وحدة التقسيم:

يجري في هذه الوحدة تقسيم الصورة الواضحة بقياس 256×256 بيكسل أو أي جزء منها، إلى أربع مصفوفات مربعة، تُمثل هذه المصفوفات دخلاً لوحدة المسح، ويجري معالجتها في وحدة المسح وفق ترتيب محدد تبعاً لمخطط التقسيم، بحيث تجري قراءة المخطط التالي في وحدة قراءة المفتاح، وتطبيقه على مصفوفة المعطيات الموافقة.



الشكل (10.2) المخطط التدفقي لمحاكاة التعمية باستخدام خوارزمية المسح SCAN ضمن بيئة MATLAB.

2.4.2- المخطط التدفقي لفك التعمية

يتألف المخطط التدفقي لعملية محاكاة فك التعمية باستخدام خوارزمية المسح من الأجزاء التالية:

أ- وحدة تحصيل الصورة:

تقوم هذه الوحدة بتحصيل الصورة المعمّاة التي قياسها 256×256 بيكسل.

ب-وحدة قراءة مفتاح التعمية العكسية:

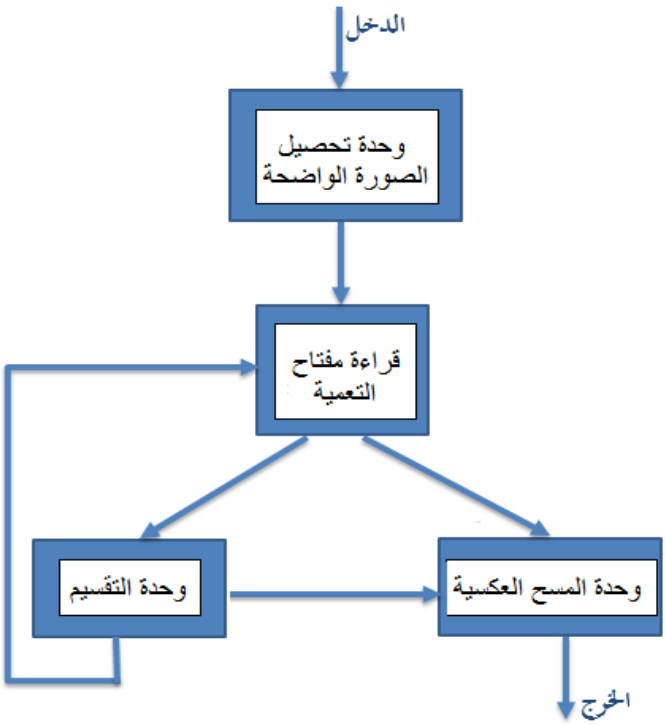
تجري قراءة مفتاح التعمية بطريقة معاكسة لعمل وحدة قراءة المفتاح في الاتجاه المباشر (أي عند التعمية). أي تُستخرج مخططات المسح الأولية ومخططات التقسيم المستخدمة في عملية التعمية، ثم يجري استنتاج المخططات المعاكسة (التي عملها يعاكس عمل المخططات الأولية (مخططات المسح العكسية)ومخططات التقسيم (مخططات الضم))، ثم يجري استدعاؤها في عملية فك التعمية بترتيب يعاكس ترتيب استدعاء مخططات المسح الأولية ومخططات التقسيم في عملية التعمية.

ت-وحدة التقسيم:

يجري في هذه الوحدة تقسيم مصفوفة الدخل إلى أربع مصفوفات جزئية، وفقاً لمخطط التقسيم المحدد في وحدة قراءة المفتاح العكسي. تمثل هذه المصفوفات الأربعة دخلاً لوحدة المسح العكسية. ثم يجري قراءة المخطط التالي في وحدة قراءة المفتاح العكسية، وتطبيقه على مصفوفة المعطيات المعمّاة الموافقة.

ث-وحدة المسح العكسية:

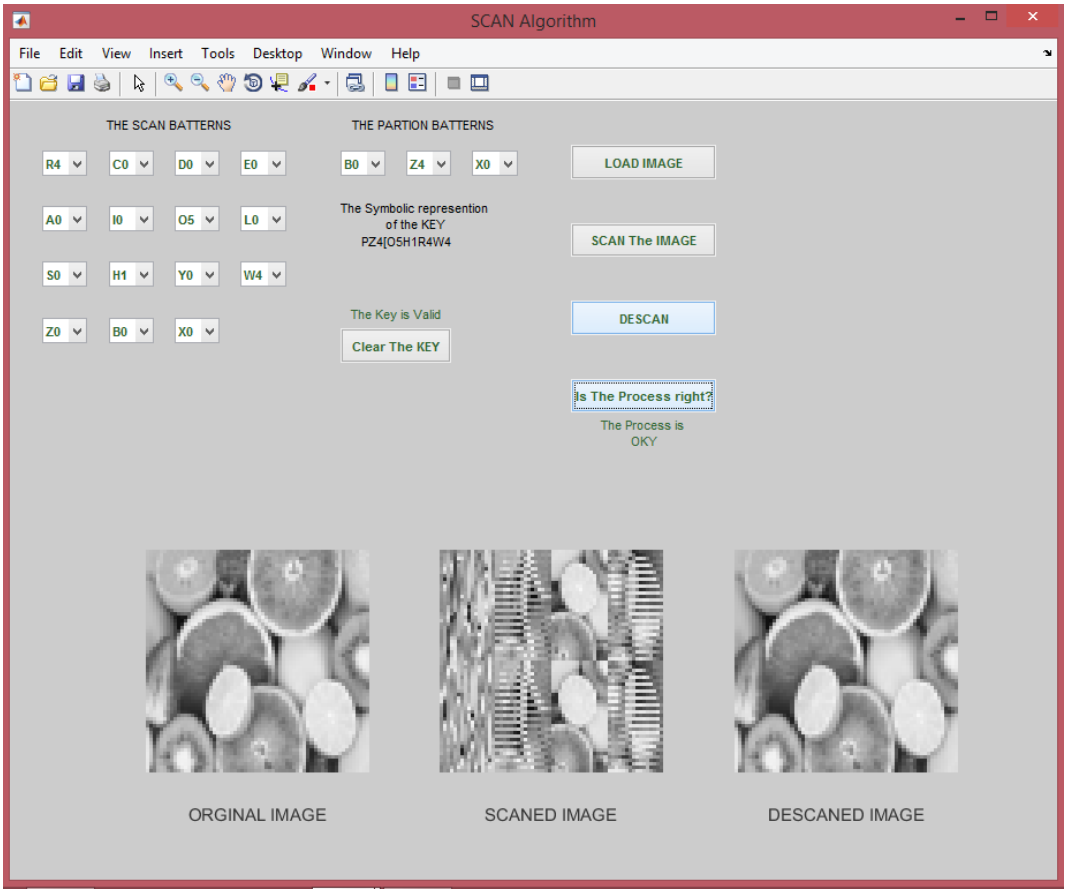
تقوم هذه الوحدة بفك تعمية الصورة المعمّاة بقياس 256×256 بيكسل أو جزء منها. دخل هذه الكتلة هو الصورة المعمّاة بالإضافة إلى نوع مخطط المسح الأولي ورقم التحويل المطبق عليه، ولها خرج وحيد هو مصفوفة الصورة الواضحة، الذي له نفس حجم صورة الدخل المعمّاة.



الشكل (11.2) المخطط التدفقي لمحاكاة فك التعمية باستخدام خوارزمية المسح SCAN على MATLAB.

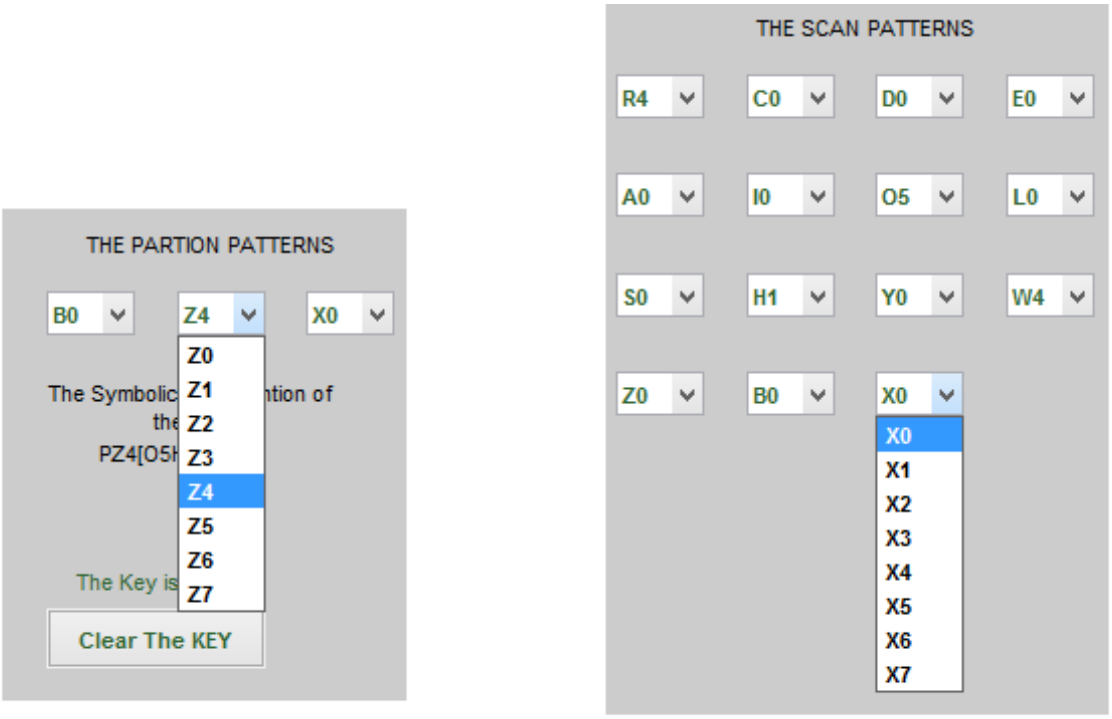
5.2- نتائج محاكاة الخوارزمية

يظهر الشكل (12.2) واجهة محاكاة خوارزمية المسح SCAN باستخدام MATLAB، والتي تتضمن كلّ من عمليتي التعمية وفك التعمية، وفيها جرى تعمية وفك تعمية صورة، وذلك باستخدام مفتاح تعمية بسيط جداً. تعرض هذه الواجهة الصورة الأصلية والصورة المعمّاة بالمفتاح السري (أي نتيجة المسح بمخطط المسح المعمّم)، والصورة المستعادة بعد عملية فك تعمية الصورة المعمّاة بمفتاح التعمية (أي نتيجة المسح العكسي بمخطط المسح المعمّم نفسه).



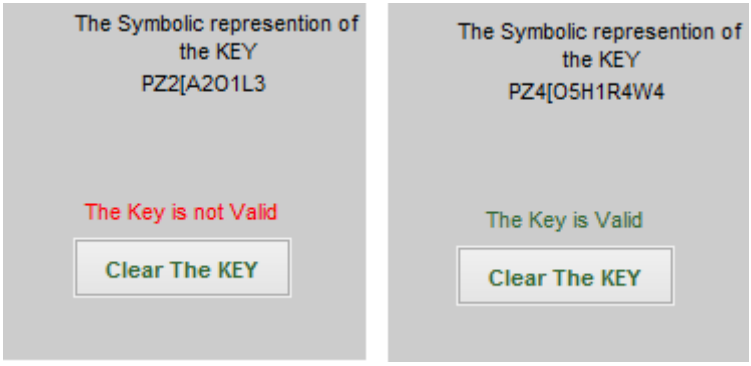
الشكل (12.2) الواجهة الرئيسية لمحاكاة خوارزمية المسح.

تسمح الواجهة الأساسية لبرنامج المحاكاة باختيار أي مخطط من مخططات المسح الأولية أو مخططات التقسيم، يظهر الشكل (13.2-a) مخططات المسح الأولية، وكيفية اختيار رقم التحويل لمخطط المسح الأولي. يُظهر الشكل (13.2-b) مخططات التقسيم وكيفية اختيار رقم التحويل المراد. وتعرض واجهة المستخدم أيضاً مفتاح المسح المعمّم أثناء تشكيله، حيث جرى تمثيله بسلسلة رموز، بحيث يشير حرف P قبل رمز المخطط إلى أنّه مخطط تقسيم وليس مخطط مسح أولي، وفي كل مرحلة يتم فحص مفتاح التعمية، والتأكد من صلاحيته. يُظهر الشكل (14.2) مفتاح التعمية كما يظهر في واجهة المستخدم، حيث المفتاح على على يمين هذا الشكل صالح ليكون مخطط مسح معمّم (أي صالح ليكون مفتاح سري)، بينما المفتاح على يسار الشكل غير صالح. تسمح هذه الواجهة بتحديد الصورة المراد تعميتها وإعطاء أمر التعمية وفك التعمية. أظهرت هذه المحاكاة صلاحية خوارزمية المسح في تعمية وفك تعمية عدد من الصور من أجل مفاتيح تعمية متنوعة.



-a- -b-

الشكل (13.2)، (a) مخططات المسح الأولية في واجهة المستخدم ، (b) مخططات التقسيم في الواجهة.



الشكل (14.2) مخطط المسح المعمّم (مفتاح التعمية) في واجهة المستخدم.

الفصل الثالث

مقارنة أداء خوارزمية المسح SCAN مع أداء الخوارزمية المعيارية AES

يقدّم الفصل الثالث لمحة موجزة عن خوارزمية التعمية المعيارية AES، وتوصيف لبعض اختبارات العشوائية المشهورة والتي تقيس أداء خوارزميات التعمية، من حيث عشوائية النص المعمّى وعلاقته بالنص الواضح، بالإضافة إلى مقارنة عدد المفاتيح المتاحة ونتائج تطبيق اختبارات العشوائية على كلّ من خوارزمية التعمية المعيارية AES وخوارزمية المسح SCAN المدروسة في هذه الاطروحة.

1.3- مقدمة

تمثل خوارزمية التعمية AES المعيار العالمي للتعمية، حيث تمثل الخوارزمية المسخدمة عالمياً من قبل معظم المنظمات والشركات والهيئات حول العالم، وعند دراسة أي خوارزمية تعمية لا بد من مقارنة أدائها مع أداء الخوارزمية المعيارية، وذلك لمعرفة جدوى استخدام هذه الخوارزمية وفعاليتها.

قبل البدء بتصميم خوارزمية المسح SCAN وبناء كيانها الصلب، جرت محاكاة خوارزمية المسح SCAN باستخدام MATLAB، كما جرى تنفيذ اختبارات العشوائية، وتطبيقها على كلّ من خوارزمية التعمية المعيارية وخوارزمية المسح SCAN، ثم جرت مقارنة أدائي الخوارزميتين، وذلك من خلال قياس عدد من المعاملات المرتبطة بقوة التعمية، بالإضافة إلى حساب عدد مفاتيح التعمية المتاحة لكل منهما. ونتج عن هذه الاختبارات صلاحية خوارزمية المسح SCAN لاستخدامات التعمية الشخصية والتجارية، مع مراعاة بعض القيود الإضافية.

يجدر الذكر أنّه جرى تنفيذ خوارزمية المسح SCAN بدون إضافة العشوائية، أي بدون تغيير قيم بيكسلات الصورة، والاكتفاء بتغيير طريقة تموضع هذه البيكسلات.

2.3- لمحة عن خوارزمية التعمية المعيارية

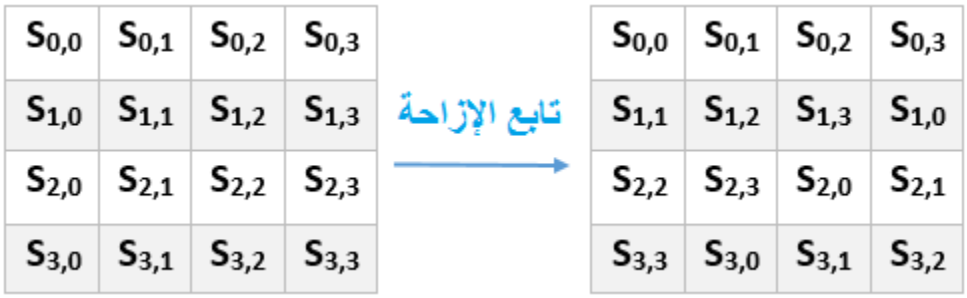
تعتبر الخوارزمية المعيارية AES من خوارزميات التعمية الكتلية المتناظرة [6]. يأخذ المفتاح السري لهذه الخوارزمية أحد القيم التالية: 128-bits, 192-bits, 256-bits. يجري تنفيذ هذه الخوارزمية من خلال عدد من الدورات، يبلغ عددها 10 أو 12 أو 14 وفقاً لطول المفتاح السري: 128-bits أو 192-bits أو 256-bits على الترتيب. يجري انطلاقاً من المفتاح السري توليد مجموعة من المفاتيح الجزئية عددها يساوي عدد الدورات ويبلغ طول كل مفتاح جزئي 128-bits. تقسم المعطيات إلى كتل طولها 128-bits ويجري التعامل مع كل كتلة معطيات كمصفوفة بقياس 4×4 bytes.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

الشكل (1.3) مصفوفة التبديل S-box [6].

تتألف كل دورة من المراحل التالية:

- المرحلة الأولى: يجري في هذه المرحلة تبديل قيمة كل بايت من كتلة المعطيات. يتألف كل بايت بالترميز الست عشري من رمزين، يجري استخدامهما كعنواني السطر والعمود في مصفوفة التبديل المبينة في الشكل (1.3). ويتم استبدال كل بايت (عنوان) بالمحتوى الموافق له في مصفوفة التبديل، فمثلاً إذا كانت قيمة البايت "7f"، فإنها تصبح بعد التبديل "d2".
- المرحلة الثانية: تقوم هذه المرحلة على إزاحة أسطر المصفوفة 4×4 الناتجة عن المرحلة الأولى دورانياً نحو اليسار. حيث يبقى السطر الأول على حاله، ويُزاح السطر الثاني بمقدار بايت واحد، ويُزاح السطر الثالث بمقدار بايتين، ويُزاح السطر الرابع بمقدار ثلاثة بايتات، يُظهر الشكل (2.3) تابع الإزاحة المستخدم في الخوارزمية المعيارية.



الشكل (2.3) الإزاحة الدورانية في خوارزمية التعمية المعيارية AES.

- المرحلة الثالثة: يجري في هذه المرحلة مزج الأعمدة، وذلك عن طريق ضرب المصفوفة 4×4 الناتجة عن المرحلة السابقة بمصفوفة معيارية، تسمى مصفوفة مزج الأعمدة.

نلاحظ من قيم عناصر مصفوفة مزج الأعمدة، الموجودة في الشكل (3.3). أنه يجب تنفيذ عمليات ضرب لعناصر المصفوفة الناتجة عن المرحلة السابقة بـ2 وبـ3. ومن الواجب ذكره أن عمليات الضرب تتم في الحقل GF(8)، وفي هذا الحقل تُعرّف عملية الضرب بـ2، بأنها إزاحة نحو اليسار، ثمّ (XOR) مع البايت الذي يأخذ القيمة (1B)، في حال كان البت MSB غير معدوم. كما يوضح الرماز الموجود في الشكل (4.3). وتُعرَّف عملية الضرب بـ3 بأنها الضرب بـ2، بالإضافة لعملية (XOR) مع القيمة الأصلية نفسها، كما يوضّح الرماز الموجود في الشكل (5.3).

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

الشكل (3.3) مصفوفة مزج الأعمدة.

```
---Multiply by 2 in the Galois Field is done with a left shift and a conditional XOR with X"1B" if the MSB is 1
    IF (a0(7) = '1') then      ---Each byte is it's own conditin
        a0x2 <=(a0(6 downto 0) & '0') XOR X"1B";
    ELSE
        a0x2 <= a0(6 downto 0) & '0';
    END IF;
```

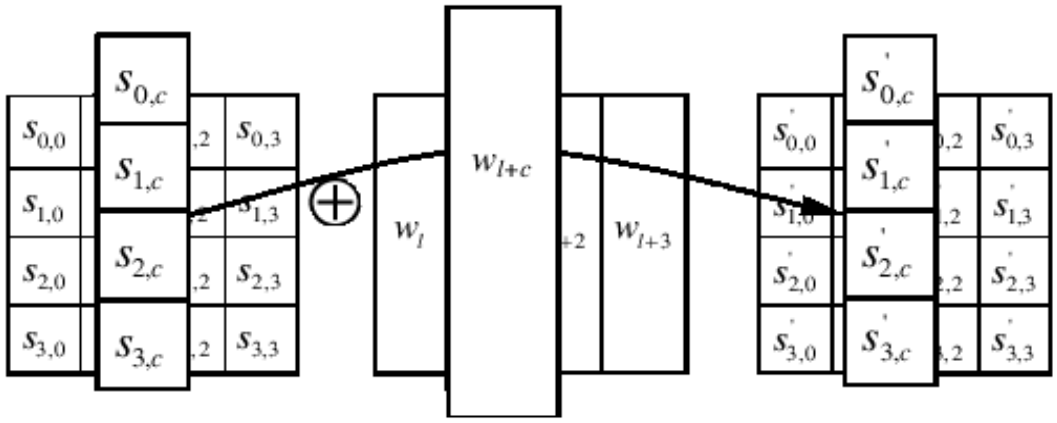
الشكل (4.3) الضرب بـ2 في الحقل GF(8).

```
--Multiply by 3: Multiply by 3 is done by first doing the Multiply by 2 and then XOR with (equivalent to adding) the original value
a0x3 <= a0x2 XOR a0;
a1x3 <= a1x2 XOR a1;
a2x3 <= a2x2 XOR a2;
a3x3 <= a3x2 XOR a3;
```

الشكل (5.3) الضرب بـ3 في الحقل GF(8).

- المرحلة الرابعة: تقوم هذه المرحلة على جمع المصفوفة الناتجة عن المرحلة السابقة، مع المفتاح الجزئي للدورة الحالية، ويجري تنفيذ عملية الجمع عن طريق عملية XOR بسيطة بين بتات المصفوفة الناتجة عن المرحلة السابقة وبتات المفتاح الجزئي الموافق.

بحيث نقسّم المفتاح الجزئي (ذو الطول 128 بت) إلى أربع كلمات (Words)، كل منها مؤلَّف من أربع بايتات، تجمع مع عمود من المصفوفة. والشكل (6.3) يُظهِر عملية إضافة مفتاح جزئي إلى مصفوفة الحالة.



الشكل (6.3) إضافة المفتاح الجزئي الموافق إلى مصفوفة 4×4 الناتجة من المرحلة السابقة.

يتم إجراء الدورات ومراحل كل دورة بشكل معاكس عند فك التعمية.

3.3- مقارنة عدد المفاتيح المتاحة في كلا الخوارزميتين AES وSCAN

بالنسبة لخوارزمية المسح، نفترض أن أبعاد الصورة N×N وأن $N = 2^m$ علماً أن m عدد طبيعي. يجري حساب عدد المفاتيح الممكنة بطريقة عودية. فمن أجل $m > 1$، يمكننا أما تقسيم الصورة إلى أربعة أجزاء وفقاً لإحدى مخططات التقسيم الثلاثة وأحد التحويلات الثمانية المتعلقة بكل مخطط، أو القيام بمسح الصورة وفقاً لإحدى مخططات المسح الخمسة عشر وأحد التحويلات الثمانية المتعلقة بكل مخطط. في حال تقسيم الصورة إلى أربعة أجزاء، تتكرر نفس الاحتمالات من أجل كل جزء من الأجزاء الأربعة التي يصبح أبعاد كل منها $\frac{N}{2} \times \frac{N}{2}$. أما من أجل $m = 1$ أي $N = 2$ تصبح احتمالات التقسيم هي نفسها احتمالات المسح أي يوجد 24 = 8×3 مفتاحاً مختلفاً. وبشكل عام يمكن أن نعبّر عن عدد المفاتيح K_N كما يلي:

$$K_N = \begin{cases} 1 & : m = 0 \\ 24 & : m = 1 \\ 15\times 8 + 3\times 8\times K_{\frac{N}{2}}^{4} & : m > 1, N = 2^m \end{cases}$$

يظهر الجدول (1.3) عدد المفاتيح المتاحة في خوارزمية المسح من أجل أبعاد مختلفة للصورة وعدد المفاتيح المتاحة في خوارزمية AES بحسب طول المفتاح.

أبعاد الصورة	مراحل التقسيم الممكنة	عدد المفاتيح الممكنة
$1*1$	0	1
$2*2$	1	24
$4*4$	2	8.0E+6
$8*8$	3	9.6E+28
$16*16$	4	2.1E+117

طول المفتاح	عدد المفاتيح الممكنة
128	2^{128} = 3.4E+38
192	2^{192} = 6.3E+57
256	2^{256} = 1.6E+77

الجدول (1.3) عدد المفاتيح الممكنة في خوارزمية المسح (إلى اليمين) وفي الخوارزمية AES (إلى اليسار).

نلاحظ أنه من أجل صورة صغيرة نسبياً بحجم 16×16، يصبح عدد المفاتيح المتاحة في خوارزمية المسح أكبر بكثير من نظيره في الخوارزمية AES من أجل أطول مفتاح فيها.

4.3- بعض الاختبارات المستخدمة لقياس أداء خوارزميات التعمية

توجد العديد من الاختبارات التي تهدف إلى قياس أداء خوارزمية التعمية، من ناحية المواصفات العشوائية للنص المعمى أو الصورة المعماة، أو من ناحية علاقة النص المعمى (الصورة المعماة) بالنص الواضح (الصورة الأصلية) وبمفتاح التعمية. كما تدل بعض المعاملات على حساسية خوارزمية التعمية لتغيرات النص الواضح ولتغيرات مفتاح التعمية. نرمز بـ C, P للنص الواضح (الصورة الأصلية) والنص المعمى (الصورة المعماة) على الترتيب. ويدل C(i,j), P(i,j) على قيمة البيكسل بالموقع (i,j) في كلا الصورتين C, P. نستعرض فيما يلي المعاملات التي جرى استخدامها لقياس أداء الخوارزميتين: SCAN, AES.

- قيمة الخطأ التربيعي الأصغري The Mean Square Error

يدل هذا المعامل على قيمة الخطأ التربيعي بين الصورة الأصلية والصورة المعماة والذي يعبر عن المسافة الإقليدية بين الصورتين. ويعطى بالعلاقة:

$$MSE = \frac{1}{T} \sum_{i,j} [P(i,j) - C(i,j)]^2$$

حيث تمثل T العدد الكليّ للبيكسلات في الصورة الواضحة أو المعمّاة. كلما زادت قيمة المعامل MSE كلما ازدادت صعوبة اكتشاف العلاقة بين الصورة الأصلية والصورة المعماة مما يحسن من أداء الخوارزمية.

- معامل التشابه البنيوي Structural Similarity Index Measure

يقدم معامل التشابه البنيوي دلالة أكبر من المعاملين السابقين، فهو يقوم بتقدير الخطأ المطلق بين الصورة الواضحة والصورة المعماة ويعطى بالعلاقة:

$$SSIM(P,C)=\frac{\left(2\mu_P\mu_C+(k_1L)^2\right)\left(2\sigma_{PC}+(k_2L)^2\right)}{\left(\mu_P^2+\mu_C^2+(k_1L)^2\right)\left(\sigma_P^2+\sigma_C^2+(k_2L)^2\right)}$$

حيث:

- ⇦ μ_P, μ_C متوسط قيم بيكسلات الصورة الواضحة والصورة المعمّاة على الترتيب.
- ⇦ σ_P^2, σ_C^2 تشتت قيم بيكسلات الصورة الواضحة والصورة المعمّاة على الترتيب.
- ⇦ σ_{PC} التغاير بين الصورة الواضحة والصورة المعمّاة، ويعطى بالعلاقة: $\sigma_{P,C}=E\left[\left(P-E(P)\right)\left(C-E(C)\right)\right]$. يعبر E عن التوقع الرياضي.
- ⇦ L المجال الديناميكي لتغير قيم بيكسلات الصورة وغالباً ما يكون 2^n-1، حيث n عدد البتات المستخدمة لتمثيل البيكسل الواحد.
- ⇦ $k_1=0.01, k_2=0.03$ هي ثوابت معيارية.

- نسبة عدد البيكسلات المتغيرة Number of Changing Pixels Rate

يستخدم هذا المعامل من أجل قياس قوة خوارزمية التعمية ضد الهجوم التفاضلي Differential Attack [7]. كلما ازدادت هذه النسبة زادت ممانعة الخوارزمية لهذا النوع من الهجمات، وبالتالي ازداد مستوى الأمان.

ولحساب نسبة البيكسلات المتغيرة نحتاج إلى تعريف المصفوفة D، كما يلي:

$$D(i,j)=\begin{cases}0, & if\ \ P(i,j)=C(i,j)\\ 1, & if\ \ P(i,j)\neq C(i,j)\end{cases}$$

وتعطى نسبة البيكسلات المتغيرة بالعلاقة التالية:

$$NCPR(P,C)=\sum_{i,j}\frac{D(i,j)}{T}\times 100\%$$

حيث يمثل T العدد الكلي لبيكسلات الصورة. كلما اقترب معامل NCPR من الواحد، كلما تحسن أداء خوارزمية التعمية.

- الكثافة المتوسطة الموّحدة المتغيرة Unified Averaged Changed Intensity

يسمح هذا المعامل بالإضافة إلى المعامل السابق NCPR بقياس قوة خوارزمية التعمية ضد الهجوم التفاضلي. تزداد قوة الخوارزمية بزيادة قيمة هذا المعامل [7]. يتم حساب هذا المعامل بالعلاقة التالية:

$$UACI(P,C)=\sum_{i,j}\frac{|P(i,j)-C(i,j)|}{F.T}\times 100\%$$

حيث يمثل F قيمة أكبر بيكسل في الصورة المعمّاة.

نلاحظ أن المعامل NCPR يعنى بعدد البيكسلات المتغيرة عند حدوث الهجوم التفاضلي، بينما يتعلق المعامل UACI بمتوسط الفرق بالقيمة المطلقة بين بيكسلات كل من الصورة الأصلية والصورة المعماة.

- تشابه جاكارد Jaccard Similarity

يقيس معامل جاكارد [8] مقدار التشابه بين صورتين مختلفتين، ويعطى بالعلاقة

$$JACSIM\ (P,C) = \frac{|X_P \cap X_C|}{|X_P \cup X_C|} = \frac{|X_P \cap X_C|}{|X_P| + |X_C| - |X_P \cap X_C|}$$

يمثل X_c, X_p مجموع قيم بيكسلات الصورة الواضحة والصورة المعماة على الترتيب.

تقوم العملية |.| بحساب عدد عناصر المجموعة. وبالتالي يعبر معامل جاكارد عن نسبة عدد القيم المتماثلة للبيكسلات في الصورتين الواضحة والمعمّاة، إلى عدد القيم المتماثلة والمختلفة للبيكسلات ضمن الصورتين.

نريد أن يكون التشابه بين الصورة الواضحة والصورة المعمّاة أقل ما يمكن، لذلك كلما نقص معامل جاكارد، كلما تحسن أداء خوارزمية التعمية.

- معامل الانزياح الزمني الديناميكي Dynamic Time Warping

يقيس هذا المعامل المسافة الأقليدية الصغرى بين الصورة الواضحة والصورة المعمّاة، بعد تطبيق انزياحات مختلفة على الصورة المعمّاة. كلما زادت قيمة هذا المعامل كلما تحسن أداء الخوارزمية.

- معامل الترابط Correlation

يقيس معامل الترابط التشابه بين الصورتين الواضحة والمعمّاة، ومن أجل تعمية جيدة يجب أن يكون الترابط بين الصورة الواضحة والصورة المعمّاة أقل ما يمكن.

- حساسية النص الواضح و حساسية المفتاح Plain text and key Sensitivity

يقوم اختبار حساسية النص الواضح، على تغيير قيمة بت واحد من النص الواضح (الصورة الأصلية) ثم حساب النسبة المئوية للبتات المتغيرة في النص المعمى (الصورة المعماة). كذلك يقوم اختبار حساسية مفتاح التعمية، على تغيير قيمة بت واحد من مفتاح التعمية، ثم حساب النسبة المئوية للبتات المتغيرة في النص المعمى. من أجل تعمية جيدة، يجب أن يكون احتمال تغيّر أي بت من النص المعمى قريباً من النصف، عند تغيير قيمة بت واحد من النص الواضح أو من مفتاح التعمية.

5.3- التجارب والاختبارات

جرت محاكاة كل من خوارزميتي التعمية: AES, SCAN، ضمن بيئة MATLAB. جرى اختيار صور أبعادها 256×256 بيكسل لإجراء الاختبارات عليها.

يظهر الجدول (2.3) نتائج هذه الاختبارات على كل من الخوارزميتين. نلاحظ أن خوارزمية المسح تقترب من الخوارزمية المعيارية من أجل جميع الاختبارات، عدا اختباري حساسية النص الواضح وحساسية مفتاح التعمية، ويمكن ملاحظة الحساسية المنخفضة لتغيّر النص الواضح، من خلال تطبيق خوارزمية المسح على صورة بيضاء تماماً (أو أي صورة بلون واحد)، فسينتج صورة معمّاة مماثلة للصورة الواضحة.

SCAN	AES	معامل الاختبار
4.38E+03	8.91E+03	MSE
6.9E-03	2.1E-03	$SSIM$
99.37%	99.51%	$NPCR$
20.92	22.91	$UACI$
6.3E-03	4.9E-03	$JACSIM$
1.13E+03	1.69E+03	DTW
6.2E-03	2.5E-03	$Correlation$
0.01%	50.00%	Plain Text Sensitivity
3.1%	50.0%	Key Sensitivity

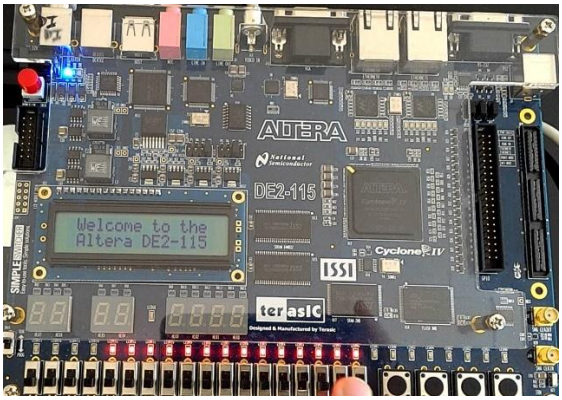
الجدول (2.3) نتائج الاختبارات على كلّ من خوارزميتي التعمية: SCAN, AES.

يمكن جعل الخوارزمية أكثر حساسيةً لتغيّر النص الواضح والمفتاح معاً، وذلك من خلال عملية إضافية، تتم بعد اجراء عملية المسح، وتتمثّل بإضافة قيم عشوائية إلى قيم بيكسلات الصورة. تكافئ هذه العملية تعمية دفقية إضافية هي التي تحمل الأمان أو يمكن أن نمتنع عن استعمال خوارزمية المسح إذا لم تتمتع الصور بمخطط تكراري مقبول.

جرى في هذه البحث محاكاة كل من خوارزميتي التعمية: AES, SCAN، ضمن بيئة MATLAB، كما جرى العديد من المقارنات والاختبارات عليهما. أظهرت النتائج أن أداء خوارزمية المسح يتقارب من أداء الخوارزمية المعيارية في معظم اختبارات الأداء، فبينما تتفوق الخوارزمية المعيارية من ناحية نتائج اختباري حساسية النص الواضح وحساسية مفتاح التعمية، فإن خوارزمية المسح تتفوق من ناحية عدد المفاتيح المتاحة، التعقيد الحسابي وسرعة المعالجة مما يمكنها من العمل بالزمن الحقيقي من أجل التعمية الفيديوية في التطبيقات التجارية والشخصية. سنرى عند تنجيز خوارزمية المسح باستخدام شريحة FPGA، أنه جرى حل مشكلة نقص الحساسية من خلال عملية إضافية هي إضافة قيم عشوائية إلى قيم بيكسلات الصورة.

الفصل الرابع

بطاقة التطوير DE2-115



يقدّم الفصل الرابع موجزاً عن تقنية بناء الكيان الصلب المستخدمة لبناء خوارزمية المسح عتادياً، حيث يقدم توصيف لبطاقة التطوير DE2-115 المستخدمة في المشروع، ويوصف كلّ من المبدّل الرقمي–التماثلي والكاميرا الرقمية المستخدمة.

1.4- مقدمة

يهدف التنفيذ العملي إلى تطبيق الدراسة النظرية والتأكد من صحة عمل الخوارزميات بالإضافة إلى تقدير تعقيد هذه الخوارزميات وسرعة عملها. تعد مرحلة التنفيذ العملي من المراحل الأساسية والصعبة للوصول إلى المنتج النهائي. عادةً ما تقتصر المشاريع على مرحلة الدراسة النظرية وتطوير الخوارزميات دون الوصول إلى منتج النهائي.

أصبح بالإمكان اليوم الوصول إلى هذه المرحلة بفضل توفر بطاقات التطوير بإمكانياتها العالية وميزاتها المتعددة كبطاقات تطوير FPGA Development Kit. جرى استخدام إحدى هذه البطاقات لتنفيذ عمليّ لخوارزمية التعمية باستخدام مخططات المسح، وهي بطاقة DE2_115 التي تحتوي على شريحة FPGA من نوع Cyclone IV E من شركة ALTERA. كما جرى اعتماد برمجيات Quartus II من شركة Altera من أجل التوصيف والإنشاء والبرمجة. أما المحاكاة فجرت باستخدام ModelSim .

يشرح هذا الفصل المنهجية العامة للتصميم باستخدام تقانة FPGA ثم يقدم البطاقة DE2_115 المستخدمة في هذا المشروع.

2.4- بطاقات FPGA

بطاقات FPGA (Field Programmable Gate Array) هي دارات متكاملة تحتوي على مصفوفة من الخلايا المنطقية المتطابقة، بحيث يوجد روابط قابلة للبرمجة بين هذه الخلايا. ويمكن للمستخدم أن يبرمج التوابع المحققة في كل خلية منطقية، كما يمكنه التحكم بالروابط بين الخلايا.

تتمتع بطاقات FPGA بعدة خصائص عامة، تتحدد هذه الخصائص بما يسمى (الحجم المنطقي للجهاز)، حيث يعبّر عن عدد البنى المنطقية الأساسية التي تحويها البطاقة، كما تتحدد خصائصها بميزات بنيتها المنطقية، وقدراتها على المعالجة، وسرعتها ومقدار استهلاكها للطاقة. وعلى الرغم من وجود أنواع كثيرة من بطاقات FPGA، فإنها تشترك في العديد من الخصائص العامة [9]:

- العناصر المنطقية: Logic Elements

تحوي جميع شرائح FPGA عدداً كبيراً جداً من العناصر المنطقية، التي تُستخدم في إنجاز تطبيق أو حل مسألة ما. ويختلف عدد العناصر المنطقية حسب نوع البطاقة المستخدمة وحسب التطبيق الذي يتم إنجازه. ويعرض الشكل (1.4) العنصر المنطقي ومكوناته.

⇦ جداول الربط:Lookup Tables

تتألف العناصر المنطقية من قلاب منطقي (flip-flop) قابل للبرمجة (واحدٍ على الأقل)، ونظام إدخال منطقي معين، ويتم غالباً التعامل مع جدول ربط مؤلف من n مدخلاً (5 على الأكثر).

⇦ موارد الذاكرة : Memory Resources

تحمل غالبية شرائح FPGA على رقاقاتها ذاكرة مدمجة بها مثل SRAM، ويمكن لهذه الذواكر أن تعمل بشكل مجموعات، ويرتبط كل عنصر للذاكرة بالذاكرة العامة المدمجة به.

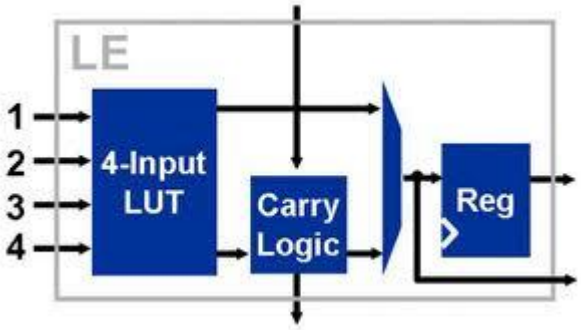
⇦ موارد التوصيل : Routing Resources

إن التوصيل هو المعيار الأساسي للمرونة التي تتمتع بها دارات FPGA. وتنطوي موارد التوصيل على مجموعة من قنوات النقل. وتقوم مفاتيح قابلة للبرمجة بربط قنوات التوصيل في دارات FPGA بعضها ببعض، أو بقنوات توصيل خارجية أخرى.

⇦ المداخل والمخارج القابلة للتشكيل Configurable I/Os:

يمكن أن تتعامل تطبيقات FPGA مع واجهات تخاطب مختلفة، ويتطلب هذا طيفاً واسعاً من المتطلبات والخصائص المعينة لبوابات دخلها وخرجها. ولذلك تتمتع هذه الدارات بخصائص عديدة لضبط هذه البوابات. فمثلاً تحوي شرائح FPGA على بوابات ذات سرعات عالية خاصة بالساعات.

يتم توصيف عمل الكيان الصلب وبرمجة شرائح FPGA باستخدام لغة تُسمّى لغة توصيف الكيان الصلب VHDL.



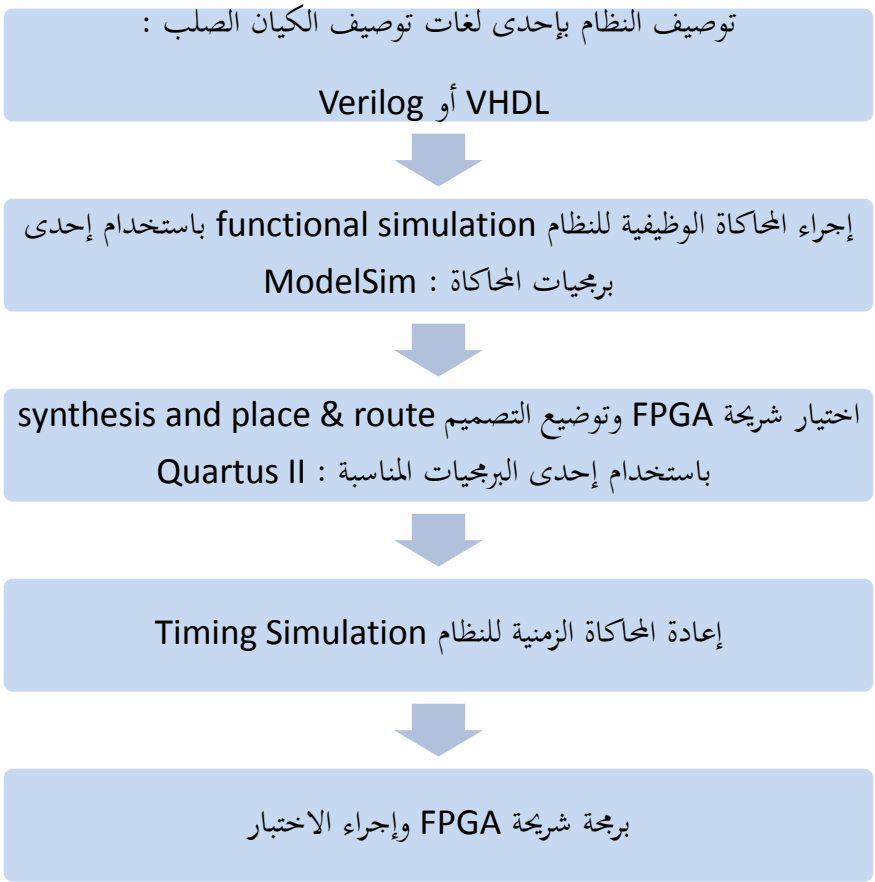
الشكل (1.4) العنصر المنطقي ومكوناته.

3.4- المنهجية العامة للتصميم باستخدام تقانة FPGA

تتألف منهجية التصميم باستخدام تقانة FPGA من عدة مراحل:

- ⇦ توصيف النظام باستخدام لغة توصيف الكيان الصلب VHDL أو باستخدام Verilog.
- ⇦ محاكاة التوصيف السابق وظيفياً باستخدام إحدى برمجيات المحاكاة، حيث تعتبر المحاكاة ضرورة للتأكد من عمل النظام ولا يمكن الاستغناء عنها، خاصةً عندما يزداد النظام تعقيداً. وتعد الأداة ModelSim من أهم برمجيات المحاكاة.
- ⇦ بعد محاكاة النظام يمكن تحويله من صيغة رمزية code إلى صيغة البوابات المنطقية Netlist. يطلق على هذه العملية تسمية الإنشاء (synthesis).
- ⇦ بعد اختيار شريحة FPGA يمكن إجراء العملية التالية وهي توضيع التصميم على هذه الشريحة (place&route). يمكن إتمام عمليات الإنشاء والتوضيع من خلال برمجيات خاصة بكل شركة FPGA. فمثلاً برمجيات شركة Xilinx هي ISE وبرمجيات شركة Altera هي Quartus II.
- ⇦ يمكن إعادة المحاكاة بإضافة الأزمنة الحقيقية والمتناسبة مع شريحة FPGA التي جرى اختيارها. في النهاية تجري برمجة الشريحة ويتم اختبار عمل النظام.

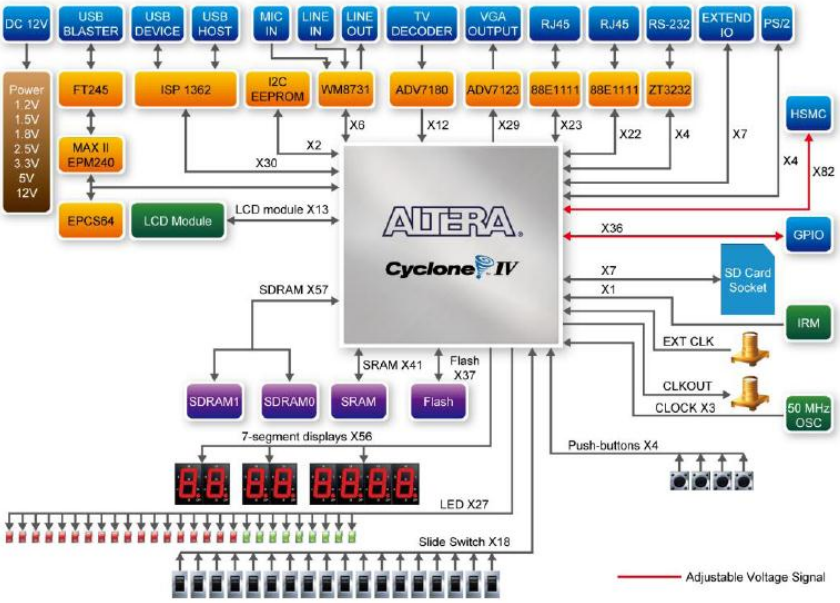
ويمثل الشكل (2.4) هذه المراحل وتتابعها.



الشكل (2.4) منهجية التصميم باستخدام FPGA.

4.4- البطاقة Altera DE2-115

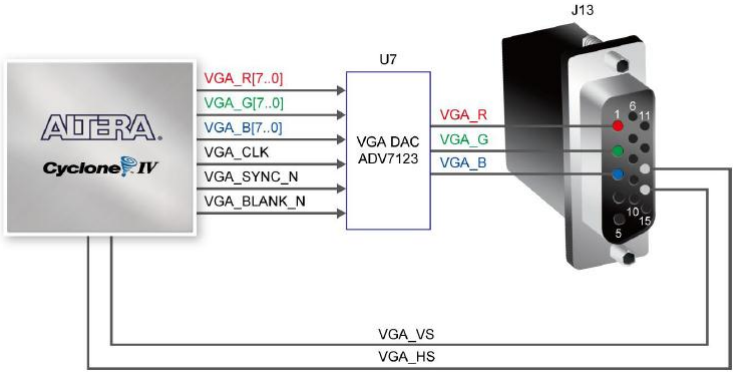
تتمتع بطاقة DE2_115 بالعديد من الميزات التي تتيح للمصمم بناء طيف واسع من الأنظمة، بدءاً من النظم البسيطة، وصولاً إلى أنظمة الصوت والصورة المعقدة. يُظهر الشكل (3.4) المخطط الصندوقي لهذه البطاقة.



الشكل (3.4) المخطط الصندوقي لبطاقات العائلة Cyclone IV E [9].

تحتوي هذه البطاقة بشكل أساسي على بطاقة FPGA من عائلة Cyclone IV E من النوع EP4CE115F29، كما تحتوي على العديد من الطرفيات، ومن هذه الطرفيات [9]:

- عدد كبير من الليدات الضوئية 18 Red LEDS, 8 Green LEDS.
- عدد من وحدات الإظهار الرقمية 7-segment displays.
- عدد من المفاتيح والأزرار : 4 Push-button, 18 Switches.
- شاشة إظهار 16×2 LCD.
- مبدّل رقمي-تماثلي: (ADV7123) VGA DAC يسمح هذا المبدل بتوليد الإشارات التماثلية للألوان الرئيسية (الأحمر، الأخضر والأزرق)، يعرض الشكل (4.4) المبدل الرقمي التماثلي VGA.



الشكل (4.4) المبدّل الرقمي-التماثلي VGA المضمّن في البطاقة DE2_115

يجري توليد إشارات التزامن الأفقي والعمودي من قِبل شريحة FPGA. يعطي الجدولان (1.4) و(2.4) المواصفات الزمنية لهاتين الإشارتين، على الترتيب [9].

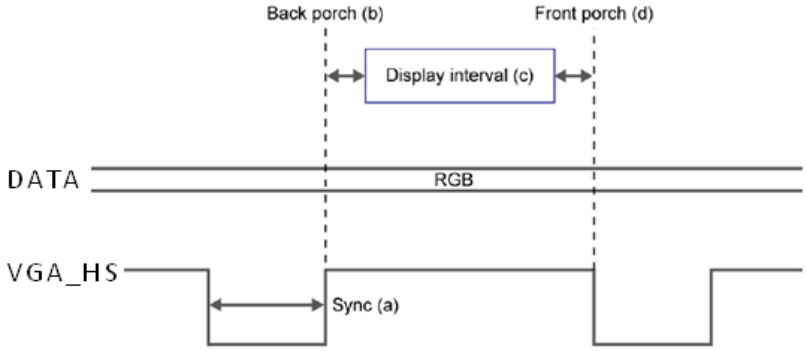
VGA mode		Horizontal Timing Spec				
Configuration	Resolution(HxV)	a(us)	b(us)	c(us)	d(us)	Pixel clock(MHz)
VGA(60Hz)	640x480	3.8	1.9	25.4	0.6	25
VGA(85Hz)	640x480	1.6	2.2	17.8	1.6	36
SVGA(60Hz)	800x600	3.2	2.2	20	1	40
SVGA(75Hz)	800x600	1.6	3.2	16.2	0.3	49
SVGA(85Hz)	800x600	1.1	2.7	14.2	0.6	56

الجدول (1.4) إشارات التزامن الأفقي.

VGA mode		Vertical Timing Spec				
Configuration	Resolution(HxV)	a(lines)	b(lines)	c(lines)	d(lines)	Pixel clock(MHz)
VGA(60Hz)	640x480	2	33	480	10	25
VGA(85Hz)	640x480	3	25	480	1	36
SVGA(60Hz)	800x600	4	23	600	1	40
SVGA(75Hz)	800x600	3	21	600	1	49
SVGA(85Hz)	800x600	3	27	600	1	56

الجدول (2.4) إشارات التزامن العمودي.

ويظهر الشكل (5.4) إشارة التزامن الأفقي. تبدأ هذه الإشارة بنبضة صفرية عرضها (a)، انظر الجدول (1.4)، وتمثل نهاية سطر من الصورة وبداية سطر جديد. يجري إظهار البيكسلات على الشاشة لفترة زمنية (c) تتعلق بعرض الصورة. تمتد هذه الفترة بعد زمن (b) من بداية سطر إلى ما قبل نهاية سطر بزمن (d)، a=3.2 us من أجل الدقة 800×600 وتردد الساعة 40 MHz، انظر الجدول (1.4). تتشكل إشارة التزامن العمودي بطريقة مشابهة لإشارة التزامن الأفقي حيث تشير النبضة الصفرية للإشارة العمودية إلى نهاية إطار صورة وبداية آخر.



الشكل (5.4) إشارة التزامن الأفقي.

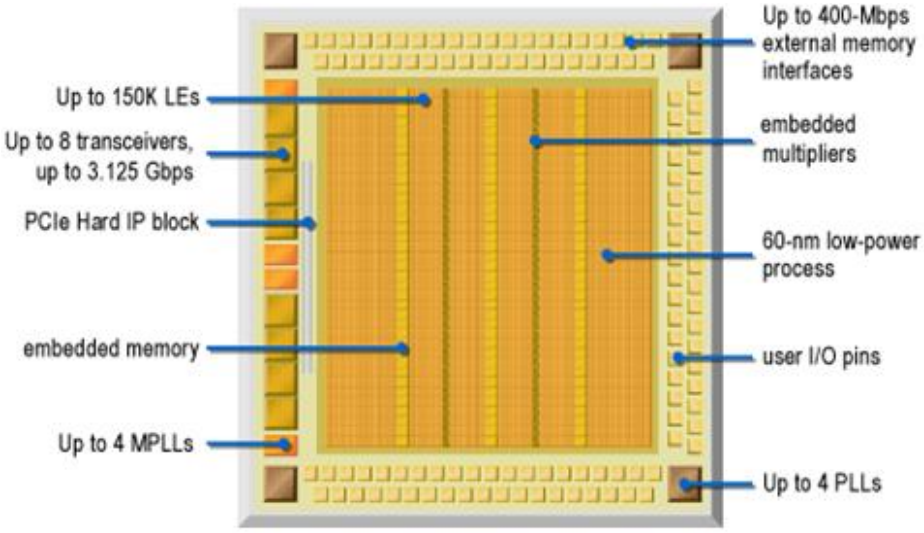
كما تحوي البطاقة ذواكر خارجية كبيرة الحجم:

- ذاكرة من نوع SRAM بحجم 2MB وعرض 16-bits. وهي ذاكرة مؤقتة، سهلة الاستخدام وتعمل بسرعات عالية : 125 MHz.
- ذاكرتان من نوع SDRAM حجم كل منهما 64MB بعرض 16-bits. الذاكرة SDRAM هي أيضاً ذاكرة مؤقتة، تتميز بأحجامها الكبيرة وتحتاج إلى بناء متحكم للتعامل معها.
- ذاكرة من نوع FLASH بحجم 8MB وعرض 8-bits. عادةً ما تستخدم هذه الذواكر لتخزين الصور والفيديو كونها تحتفظ بمحتواها بعد إيقاف التشغيل.

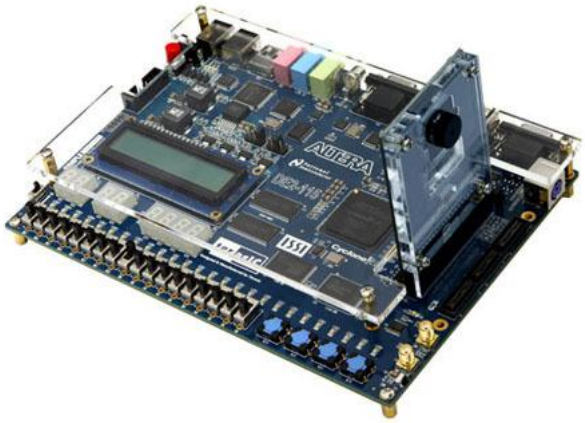
وتحتوي الشريحة EP4CE115F29 المضمنة في هذه البطاقة، يظهر الشكل (6.4) هذه الشريحة ومحتوياتها، ما يلي:

- 114480 عنصراً منطقياً Logic Elements.
- ذاكرة داخلية بحجم 3888 Kbits.
- ضوارب مضمنة 18×18 بعدد 266.
- حلقة إقفال الطور PLL عدد 4.
- 528 وحدة دخل- خرج للمستخدم.

ويمكن ربط البطاقة بكاميرا رقمية إما عن طريق مدخل الفيديو التماثلي الموصول بمفكك الترميز الفيديوي أو عن طريق وصلة خارجية كما هو وضع الكاميرا المستخدمة في مشروعنا، يوضح الشكل (7.4) ربط الكاميرا عن طريق وصلة خارجية.



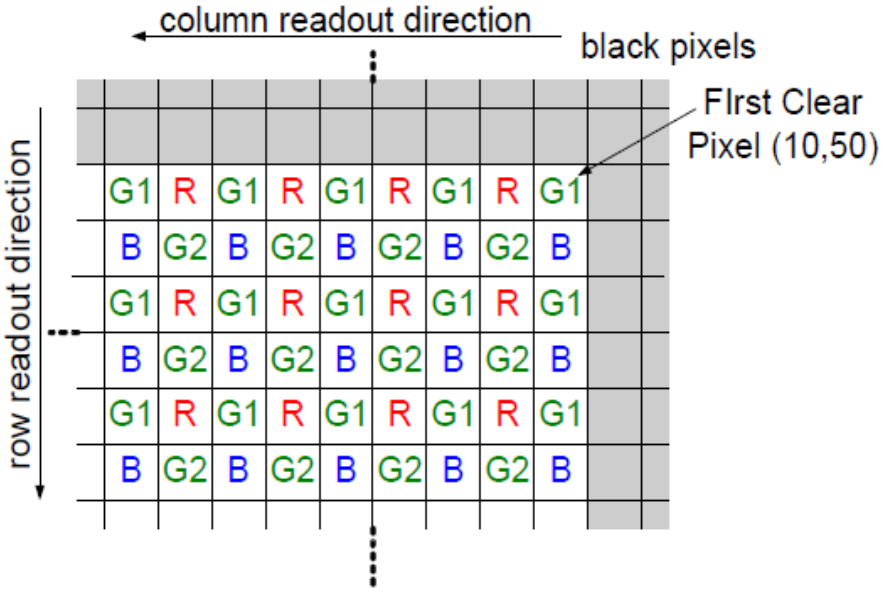
الشكل (6.4) شريحة EP4CE115F29 المضمنة في بطاقة DE2_115.



الشكل (7.4) ربط الكاميرا مع البطاقة بوصلة خارجية.

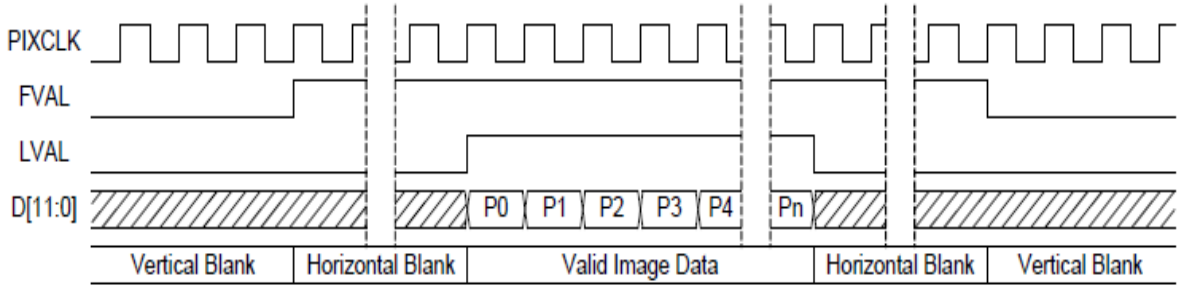
5.4- الكاميرا الرقمية TRDB_D5M

تتألف الكاميرا من مصفوفة من البيكسلات: 2752 عمود و 2004 سطر تعنون بواسطة رقم العمود والسطر، والعنوان (column 0, row 0) يمثل الزاوية العليا اليمنى للمصفوفة. يرتبط كل بيكسل بحساس ضوئي أحمر أو أخضر أو أزرق. تتوضع حساسات الألوان على شكل مصفوفة باير (Bayer Matrix)، حيث يتألف السطر الأول من تناوب بيكسلات R,G1 انظر الشكل (8.4)، ويتألف السطر الثاني من تناوب بيكسلات R,G2 وهكذا... . يمتلك اللونان G1, G2 نفس الحساس ولكن يعاملان كلونين مستقلين [10].



الشكل (8.4) توضع بيكسلات الألوان ضمن الأسطر.

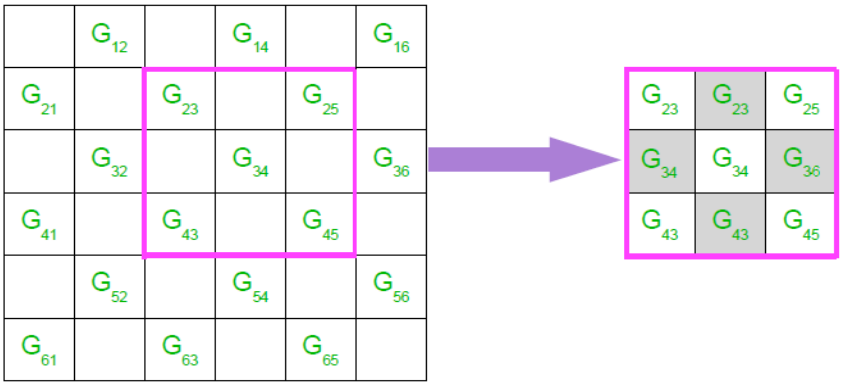
تقسم صورة الخرج إلى أطر وكل إطار يقسّم إلى أسطر. وتحدد الإشارتان LINE_VAL و FRAME_VAL حدود الأسطر والأطر على الترتيب.



الشكل (9.4) طريقة قراءة الصورة زمنياً.

تتم قراءة البيكسل Pi، كما يوضّح الشكل (9.4) من الصورة عند كل نبضة من الساعة PIXCLK عندما تكون FRAME_VAL=1 و LINE_VAL=1. ويجري تمثيل البيكسل على 12-bits.

يتألف كل بيكسل ضمن الصورة نمط RGB من ثلاثة عينات لونية (R, G, B). أما ضمن مصفوفة باير (Bayer Matrix) فكل بيكسل هو عبارة عن لون واحد فقط من الألوان (R, B, G1, G2) وبالتالي كل بيكسل ينقصه عينتان ويجب أن نقوم باستيفاء هاتين العينتين كي نحصل على البيكسل RGB. تستخدم لهذا الغرض طريقة تكرار الجار الأقرب. يوضح الشكل (10.4) مثالاً عن استيفاء اللون الأخضر الناقص في أربع بيكسلات، حيث يحل محل اللون الأخضر الناقص قيمة اللون الأخضر في البيكسل المجاور. وتطبق الطريقة ذاتها على باقي البيكسلات ومن أجل اللونين الأحمر والأزرق.

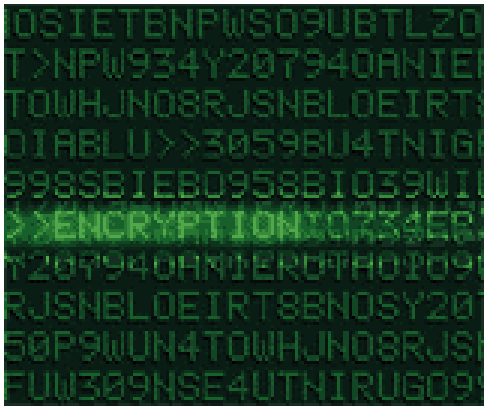


الشكل (10.4) استيفاء اللون الأخضر.

سيجري في الفصل القادم توصيف تفصيلي للكيان الصلب المنفّذ، حيث سيجري عرض التصميم المقترح لخوارزمية المسح SCAN، وطريقة تنفيذه عملياً باستخدام بطاقة DE2_115.

الفصل الخامس

بناء الكيان الصلب لخوارزمية المسح SCAN على شريحة FPGA



يقدّم الفصل الخامس خطوات بناء الكيان الصلب لخوارزمية المسح SCAN، باستخدام دارة قابلة للبرمجة FPGA، حيث يقدم المخططات التدفقية والصندوقية لمراحل بناء عتاديات الخوارزمية، وذلك في ثلاث تصاميم هي: تصميم بدون إضافة العشوائية، تصميم لتعمية الصور والتصميم النهائي لتعمية الفيديو بالزمن الحقيقي.

1.5- مقدمة

بنية التصميم المطروح في هذا العمل قادرة على مسح صور بدقة عالية في الزمن الحقيقي. على الرغم من أن خوارزمية المسح خوارزمية تعمية كتلية، وتستخدم كتلاً كبيرة نسبياً. إنّ التصميم المعروض يستخدم كتل 256×256 بيكسل لتأمين معدل معطيات معماة مناسب للعمل بالزمن الحقيقي. هذه البنية مصممة للعمل على بطاقة DE2_115 التي تحتوي على شريحة FPGA من نوع EP4CE115F29 من عائلة Cyclone IV E. جرى توصيف التصميم بلغة VHDL. أما المحاكاة فجرت باستخدام ModelSim وذلك للتحقق من عمل الخوارزمية.

2.5- الأعمال ذات الصلة

قلّة جداً من خوارزميات التعمية متخصصة بتعمية الصور، بينما العديد منها مخصص لتعمية المعطيات الأخرى. وبالعموم معظم الخوارزميات المطروحة مطبقة برمجياً وتعطي أمناً عالياً نسبياً، ولكن معدّل المعطيات المعمّاة منخفض نسبياً وذلك لا يناسب العمل بالزمن الحقيقي. ومن ناحية أخرى فإنّ عدداً قليلاً جداً من الخوارزميات المطروحة مبنيّة على عتاديات، باستخدام دارات فعلية، وهذه الخوارزميات بشكلٍ عام موجهة باتجاه التعمية الدفقية. تقدم تكنولوجيا الدارات القابلة لإعادة البرمجة FPGA توازناً بين السرعة والمرونة، وقد أثبتت أنها تكنولوجيا واعدة، ومناسبة جداً للتنفيذ العملي للخوارزميات.

جرى تنفيذ بعض خوارزميات التعمية المعروفة، مثل خوارزمية DES وخوارزمية التعمية المعيارية AES، عملياً على دارات منطقية قابلة لإعادة البرمجة، وذلك بسبب مرونتها وفعاليتها العالية والأمن الجيد الذي تقدمه.

طُرح عدد قليل جدا من خوارزميات التعمية، المخصصة لتعمية الصور. ومعظمها كان معتمداً على نظرية الفوضى، في بنية شجرية أو مفاهيم أخرى، كما جرى استخدام الخوارزمية المعيارية AES لتعمية الصور، ولكنّ التعقيد الكبير لهذه الخوارزمية واختيار كتل صغيرة نسبياً (حجم الكتلة في الخوارزمية المعيارية AES هو 16-bytes)، جعلها غير مناسبة للعمل في الزمن الحقيقي، فعلى الرغم من الأمان الكبير نسبياً الذي تقدمه هذه الخوارزمية، فإنها عجزت عن تحقيق شروط العمل في الزمن الحقيقي [1].

وبشكل عام جرى التنفيذ عتادياً لعدة خوارزميات ضغط، مثل خوارزمية MPEG، ولم يتم تنفيذ خوارزميات تعمية صورة وفيديو عتادياً.

تنتمي خوارزمية المسح إلى عائلة خوارزميات التعمية التكرارية، التي تقوم بتعمية كلّ من الصورة والفيديو. وهي تعتمد على تبديل أماكن البيكسلات، وتغيير قيمة كل بيكسل. تعتمد قوة التعمية في خوارزمية المسح على العدد الكبير لمفاتيح المسح المتاحة. عملياً، لدينا من أجل صورة قياسها 512x512 بيكسل 10^{76000} مفتاح سري ممكن [11]. وهذا يعني أن أقوى الحواسيب التفرعية حالياً تحتاج إلى ما يقارب 10^{75000} سنة لتقوم بكسر تعمية هذه الصورة باستخدام البحث الشامل (brute force). تحتوي خوارزمية المسح على جزأين هما الضغط والتعمية، ولكن قسم الضغط منها يجعلها بطيئة وغير قابلة للتنفيذ في الزمن الحقيقي، لذلك الهدف من هذا المشروع تنفيذ جزء التعمية من الخوارزمية فقط، وذلك للتمكن من العمل في الزمن الحقيقي.

الفكرة الاساسية من تطبيق خوارزمية المسح على دارة منطقية قابلة لإعادة البرمجة هي إتاحة إمكان تغيير مفاتيح التعمية بشكل مباشر. يوجد في التصميم المطروح مجموعة من المفاتيح يمكن التبديل بينها أثناء التعمية وفك التعمية. كما أن الدارات المنطقية القابلة لإعادة البرمجة تعطي إمكان الملاءمة بين المتطلبين المتعاكسين: التعقيد والسرعة.

الهدف من هذا البحث هو تقديم بنية لخوارزمية المسح تؤمن زيادة في معدل المعطيات المعماة، مع تعقيد مقبول في العتاديات. حيث جرى اختيار صور256x256 بيكسل، و8-bits لتمثيل البيكسل.

يعني العمل بالزمن الحقيقي أن النظام يحقق تدفق معطيات أكبر أو يساوي: 4 Mbit/sec (0.5 Mbyte/sec) (مثال فيديو مضغوط 640 X 480 X 16 bit MPEG2 وبتردد 25 frame/sec). هذا الأداء مقبولاً بالنسبة للتكنلوجيا الحالية [11]. أما بالنسبة لتصميمنا، فيتألف كل إطار من 256×256 بيكسل رمادي (أي byte لكل بكسل)، وهذا يعني أنّ تدفق المعطيات المعمّاة يصل إلى 13 Mbit/sec، أي أنّنا نعمل بالزمن الحقيقي.

3.5- المخطط التدفقي لخوارزمية المسح

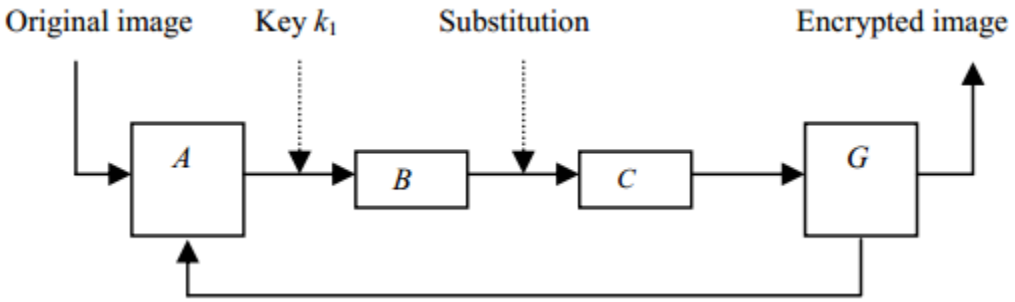
يوضح الشكل (1.5) المخطط التدفقي للتعمية باستخدام خوارزمية المسح. أولاً نقوم بتعمية الصورة الأصلية بمفتاح المستخدم K_1 (K_1 يمثل مخطط مسح معمّم، وهو المفتاح السري)، ثمّ نجري عملية تبديل لقيم بيكسلات الصورة الناتجة، يجري تغيير قيم البيكسلات وفق التحويل المعرف بالعلاقة:

$$C[i] = \left(B[i] + \left((C[i-1] + 1) * R[i]\right) \bmod 256\right) \bmod 256$$

يضمن هذا التحويل تحقق شرطي النثر والخلط (diffusion and confusion)، المعرفة وفق شانون، وهما حجرا الزاوية لتعمية كتلية جيدة.

تعني خاصة النثر diffusion أنّ تغيير محرف واحد من النص الواضح (هنا الصورة الأصلية)، يؤدّي إلى تغيّر عدّة محارف في النص المعمّى (الصورة الناتجة عن التعمية)، وبشكل مشابه، فإنّ تغيير محرف واحد في النص المعمّى يؤدي إلى تغيّر عدّة محارف في النص الواضح (الصورة الناتجة عن فك تعمية الصورة المعمّاة).[12]

بينما تعني خاصة الخلط confusion أنّ مفتاح التعمية (مخطط المسح المعمّم في خوارزمية المسح SCAN) لا يرتبط بطريقة بسيطة بالنص المعمّى. وذلك يعني عملياً أنّ كل محرف في النص المعمّى يعتمد على عدّة أجزاء من مفتاح التعمية.[12]
ويجري تحقيق هاتين الخاصتين بعملية التبديل الموجودة بين B و C في المخطط التدفقي المبيّن في الشكل (1.5)، وذلك بإضافة سلسلة قيم عشوائية منتظمة R.



الشكل (1.5) المخطط التدفقي لنظام التعمية باستخدام خوارزمية المسح.

قمنا في هذا العمل بتنفيذ تصميمين لخوارزمية المسح، يختص التصميم الأول منها بتعمية الصور، بينما يختص التصميم الثاني بتعمية المعطياة الفيديوية والتلفزية، وفي الحالتين جرت التعمية بالزمن الحقيقي.

4.5- التصميم الأول : تطبيق خوارزمية المسح على صورة بدقة 256×256 بيكسل

يُظهر الشكل (2.5) المخطط الصندوقي للتصميم الأول الذي يقوم بتطبيق خوارزمية المسح على صورة بدقة 256×256 بيكسل.

- يجري تخزين الصورة الواضحة في الذاكرة ROM. نقوم بقراءتها مرة واحدة، بعد كل تهيئة للنظام وكتابتها ضمن الذاكرة RAM1.
- تمتلك الذاكرة RAM1 بوابتين a, b، مما يسمح بإجراء عمليتي قراءة على التوازي، حيث تتم قراءة هذه الذاكرة بطريقتين:

1- وفقاً للترتيب الطبيعي، وذلك من أجل إظهار الصورة الواضحة على الشاشة، حيث تظهر المعطيات الواضحة على المخرج data_out_a_1.

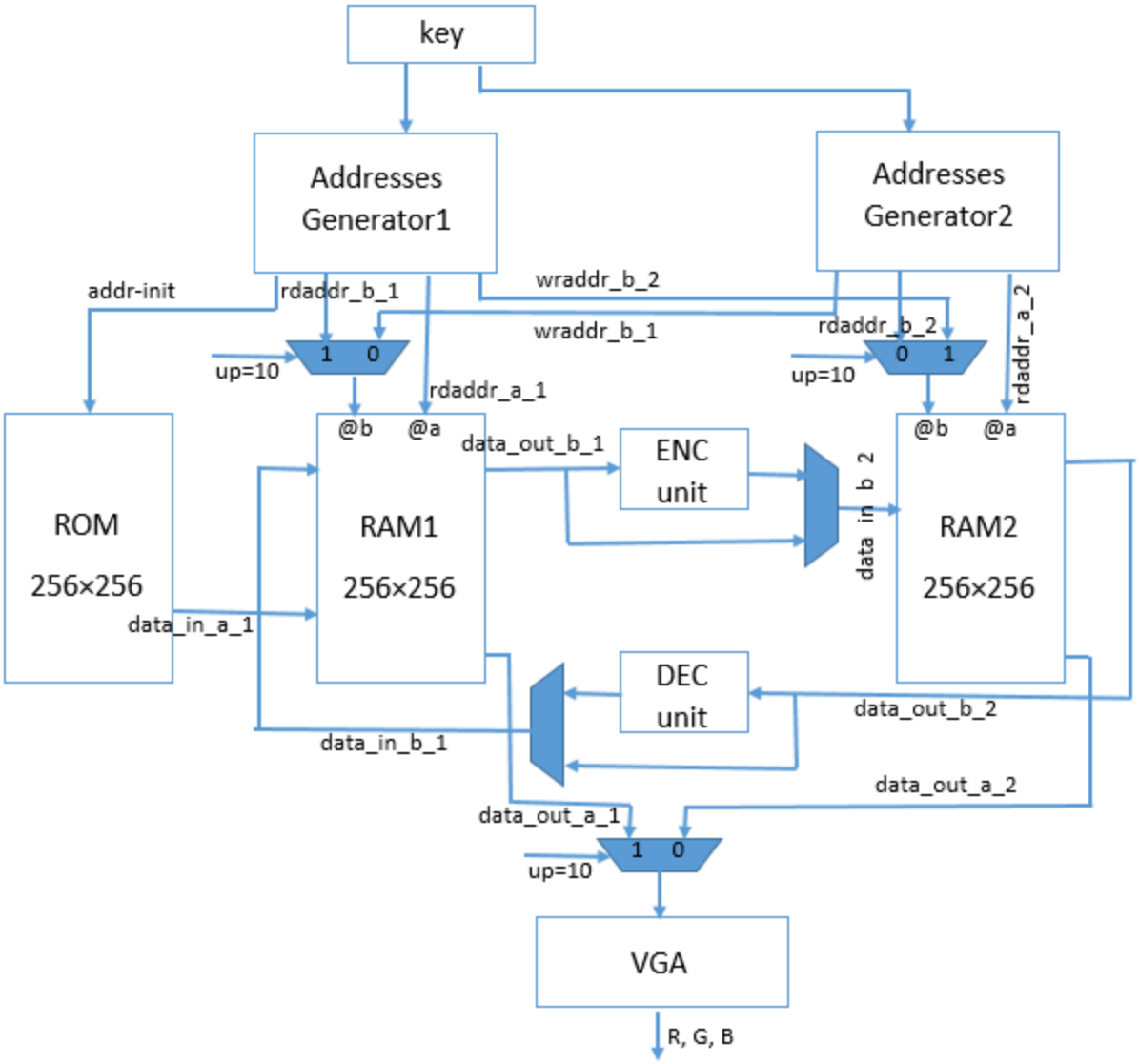
2- وفقاً لمخططات المسح الأولية والتقسيم الموافقة لمفتاح التعمية key، وذلك من أجل إعادة ترتيب مواضع البيكسلات. تظهر المعطيات على المخرج data_out_b_1. وتتم كتابة هذه المعطيات في الذاكرة RAM2، وفقاً للترتيب الطبيعي. يمكننا تبديل قيم البيكسلات باستخدام الوحدة ENC unit، والتي سنأتي على شرحها لاحقاً.

- يجري تنفيذ العمليات السابقة خلال فترة عرض النصف العلوي من الشاشة، كما هو مبين في المخطط الزمني لتوليد العناوين المبيّن في الشكل (3.5). تقوم الوحدة Addresses Generater1، والتي سنأتي على شرحها لاحقاً أيضاً، بتوليد العناوين الخاصة بهذه الفترة.
- في فترة عرض النصف السفلي من الشاشة، يجري تنفيذ العمليات التالية:

1- قراءة الذاكرة RAM2 وفقاً للترتيب الطبيعي، وذلك من أجل إظهار الصورة المعمّاة على الشاشة، تظهر المعطيات المعمّاة على المخرج data_out_a_2.

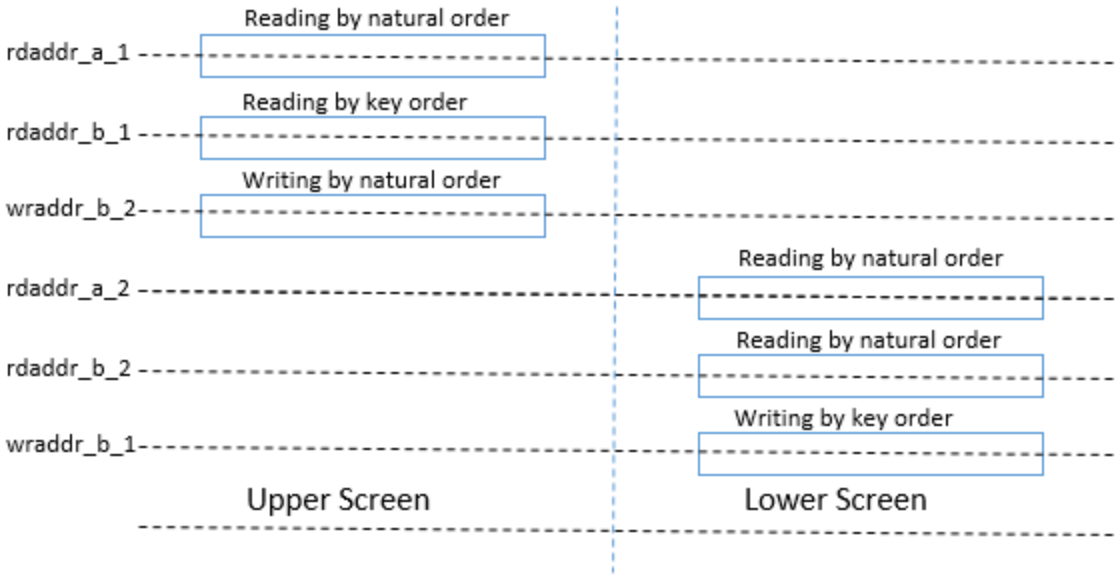
2- قراءة الذاكرة RAM2 وفقاً للترتيب الطبيعي، وإعادة كتابة المعطيات هذه المعطيات، الموجودة على المخرج data_out_b_2، في الذاكرة RAM1 لكن وفقاً لمخططات المسح الأولية والتقسم الموافقة لمفتاح التعمية key. يمكننا إعادة تبديل قيم البيكسلات باستخدام الوحدة DEC unit، والتي سنأتي على شرحها لاحقاً.

- تقوم الوحدة Addresses Generation2 بتوليد العناوين الخاصة بفترة عرض النصف السفلي من الشاشة.
- تقوم الوحدة VGA بتوليد اشارات التزامن الأفقية والعامودية بالإضافة إلى إشارات الألوان RGB اللازمة لإتمام العرض على الشاشة.



الشكل (2.5) المخطط الصندوقي للتصميم الأول الذي يقوم بتطبيق خوارزمية المسح على صورة بدقة 256×256 بيكسل.

إذاً تضم الذاكرة RAM1 الصورة الواضحة، وتضم الذاكرة RAM2 الصورة المعمّاة، وعند فك التعمية يجري إعادة كتابة الصورة الناتجة في الذاكرة RAM1، وذلك فوق الصورة الأصلية، فإذا ظهرت الصورة نفسها على خرج الذاكرة RAM1، فإنّ عمليتي التعمية وفك التعمية جرتا بشكل صحيح.



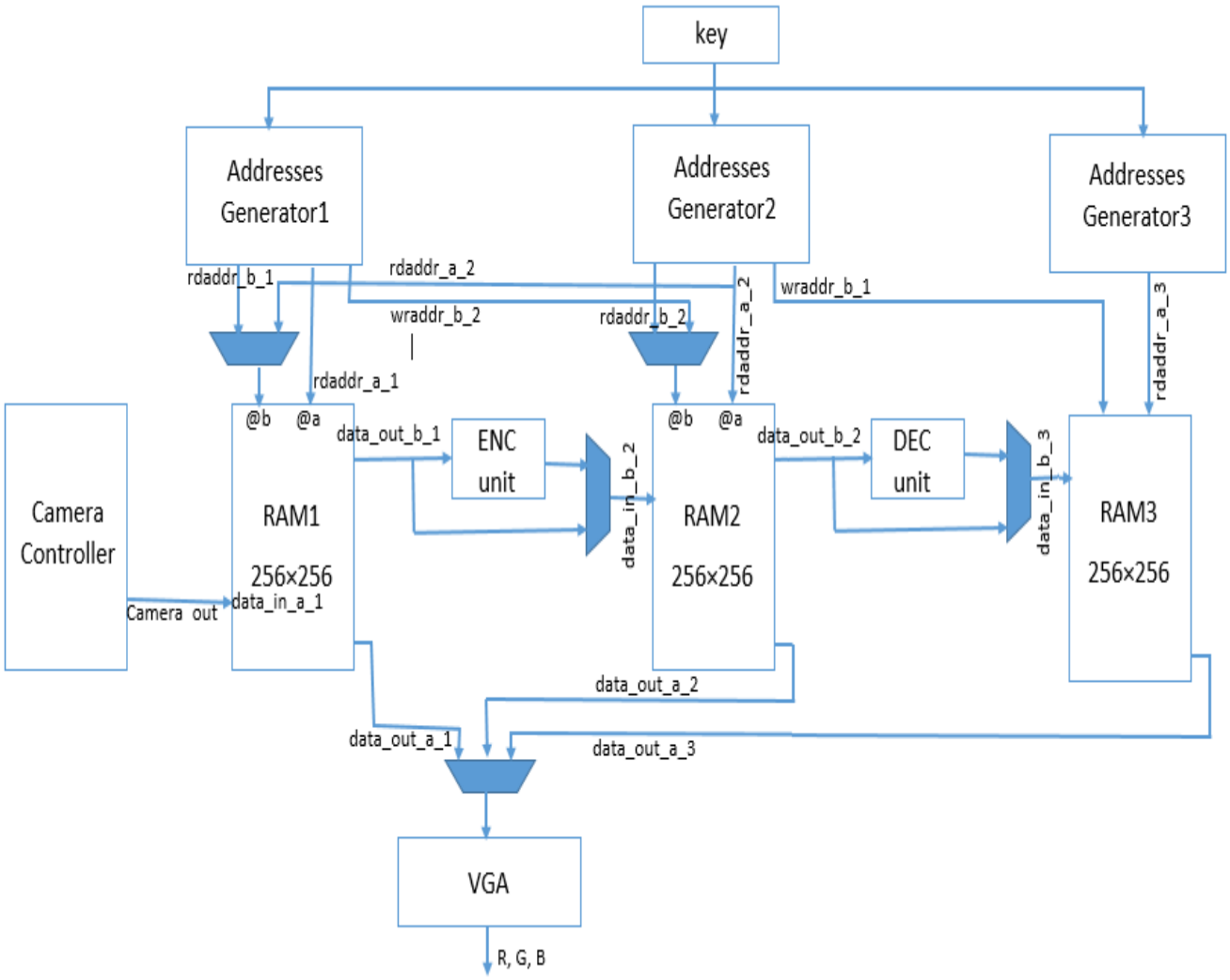
الشكل (3.5) المخطط الزمني لتوليد العناوين.

من الضروري في المرحلة الأولى التأكد من تطبيق خوارزمية المسح على صورة ثابتة، والتأكد من صحة عملها، قبل تطبيقها على سلسلة من الصور أو فيديو، الذي هو الهدف من التصميم الثاني.

5.5- التصميم الثاني : تطبيق خوارزمية المسح على فيديو بدقة 256×256 بيكسل

يُظهر الشكل (4.5) المخطط الصندوقي للتصميم الثاني، الذي يقوم بتطبيق خوارزمية المسح SCAN على فيديو بدقة 256×256 بيكسل. نلاحظ وجود تشابه كبير بين التصميمين.

- تحتوي الذاكرة RAM1 على المعطيات الفديوية الواضحة، التي يجري تحصيلها من الكاميرا، وذلك عبر الوحدة Camera-Controller، التي سنأتي على شرحها لاحقاً.
- نقوم بقراءة الذاكرة RAM1 وفقاً لمخططات المسح الأولية والتقسيم الموافقة لمفتاح التعمية key، وكتابة معطيات الخرج data_out_b_1 في الذاكرة RAM2، وفقاً للترتيب الطبيعي، وذلك خلال فترة عرض النصف العلوي من الشاشة.
- في الفترة اللاحقة (فترة عرض النصف السفلي من الشاشة)، يجري قراءة الذاكرة RAM2، وفقاً للترتيب الطبيعي، وكتابة معطيات الخرج data_out_v_2 في الذاكرة RAM3، وفقاً لمخططات المسح الأولية والتقسيم الموافقة لمفتاح التعمية key.
- يجري إظهار محتويات الذواكر الثلاثة على شاشة العرض باستخدام وحدة الإظهار VGA.



الشكل (4.5) المخطط الصندوقي للتصميم الثاني، الذي يقوم بتطبيق خوارزمية المسح SCAN على فيديو بدقة 256×256 بيكسل.

6.5- الوحدات الأساسية المكوّنة للتصميمين

يتألف التصميم الأول والثاني من عدة وحداة مشتركة، تقوم بنفس الوظيفة، وسنقدمها بالتفصيل مع شرح هدف كلّ منها:

1.6.5- وحدة توليد العناوين Addresses Generator

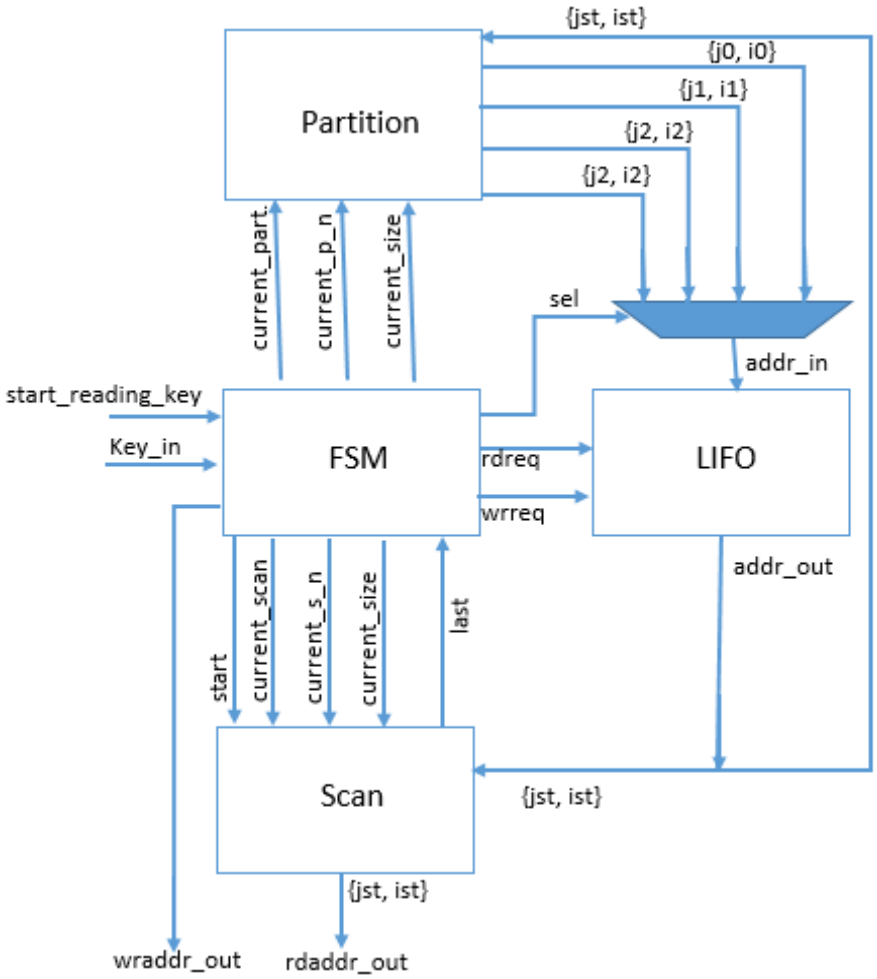
تقوم وحدة توليد العناوين بتوليد العناوين اللازمة للقراءة أو الكتابة من الذواكر، حيث تقوم الوحدة Addresses Generator1 بتوليد العناوين الخاصة بفترة عرض النصف العلوي من الشاشة، بينما تقوم الوحدة Addresses

Generator2 بتوليد العناوين الخاصة بفترة عرض النصف السفلي من الشاشة، سنقوم بشرح الوحدة الأولى فيما يلي فقط لوجود تشابه بين الوحدتين.

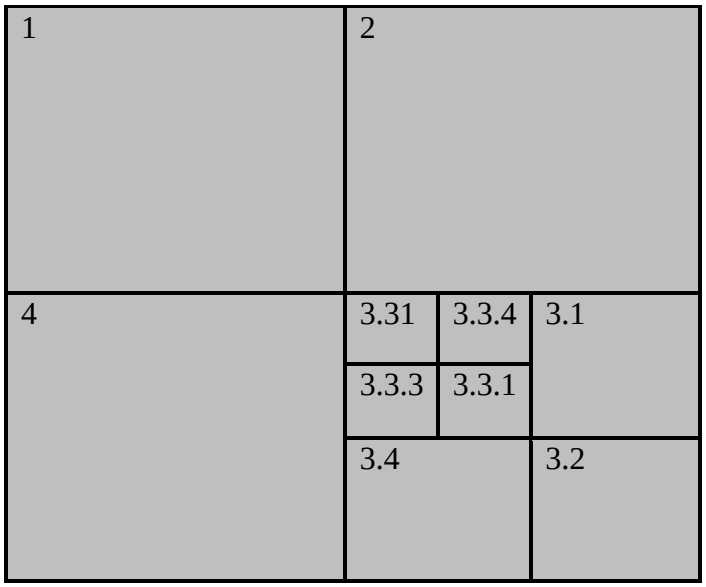
يُظهر الشكل (5.5) المخطط الصندوقي لوحدة توليد العناوين Addresses Generator1، يعتمد عمل هذه الوحدة بشكل أساسي على وحدة التحكم FSM، التي تقوم بقراءة مفتاح التعمية key_in عند وصول نبضة start_reading_key، تتم عملية تحليل المفتاح حسب القواعد المذكورة في الفقرة (3.2) في الفصل الثاني.

من أجل فهم عمل هذه الوحدة. لنأخذ مثال مخطط التقسيم المذكور في الشكل (6.5). يظهر في هذا الشكل الترتيب المتبع بحسب مفتاح التعمية، لمسح الصورة بعد تقسيمها إلى مربعات جزئية.

نعتبر أنّ كل مربع جزئي له عنوان مرجعي يحتوي رقم السطر i ورقم العمود j لرأس المربع العلوي اليساري. يتألف العنوان من 16-bits، نصفها الأدنى يمثل رقم السطر ونصفها الأعلى يمثل رقم العمود addr = {j,i}.



الشكل (5.5) وحدة توليد العناوين Addresses Generator1.



الشكل (6.5) مثال عن مخطط تقسيم لصورة بقياس 256×256.

نستخدم ذاكرة من نوع LIFO، من أجل تخزين عناوين رؤوس المربعات الجزئية، مما يتيح لنا العودة إليها عندما يحين زمن مسحها.

نبيّن فيما يلي تطور محتوى الذاكرة LIFO، تبعاً للمثال المذكور في الشكل (6.5).

1- كتابة أربعة عناوين تمثل رؤوس المربعات.

LIFO

4
3
2
1

2- مسح المربع ذو الرقم (1).

LIFO

4
3
2

3- مسح المربع ذو الرقم (2).

LIFO

4
3

4- كتابة أربعة عناوين جديدة تمثل تقسيم المربع ذو الرقم (3).

LIFO

4
3.4
3.3
3.2
3.1

5- مسح المربع ذو الرقم (3.1).

LIFO

4
3.4
3.3
3.2

6- مسح المربع ذو الرقم (3.2).

LIFO

4
3.4
3.3

7- كتابة أربعة عناوين جديدة تمثل تقسيم المربع ذو الرقم (3.3).

LIFO

4
3.4
3.3.4
3.3.3
3.3.2
3.3.1

8- مسح المربع ذو الرقم (3.3.1).

LIFO

4
3.4
3.3.4
3.3.3
3.3.2

9- مسح المربع ذو الرقم (3.3.2).

LIFO

4
3.4
3.3.4
3.3.3

10- مسح المربع ذو الرقم (3.3.3).

LIFO

4
3.4
3.3.4

11- مسح المربع ذو الرقم (3.3.4).

LIFO

4
3.4

12- مسح المربع ذو الرقم (3.4).

LIFO

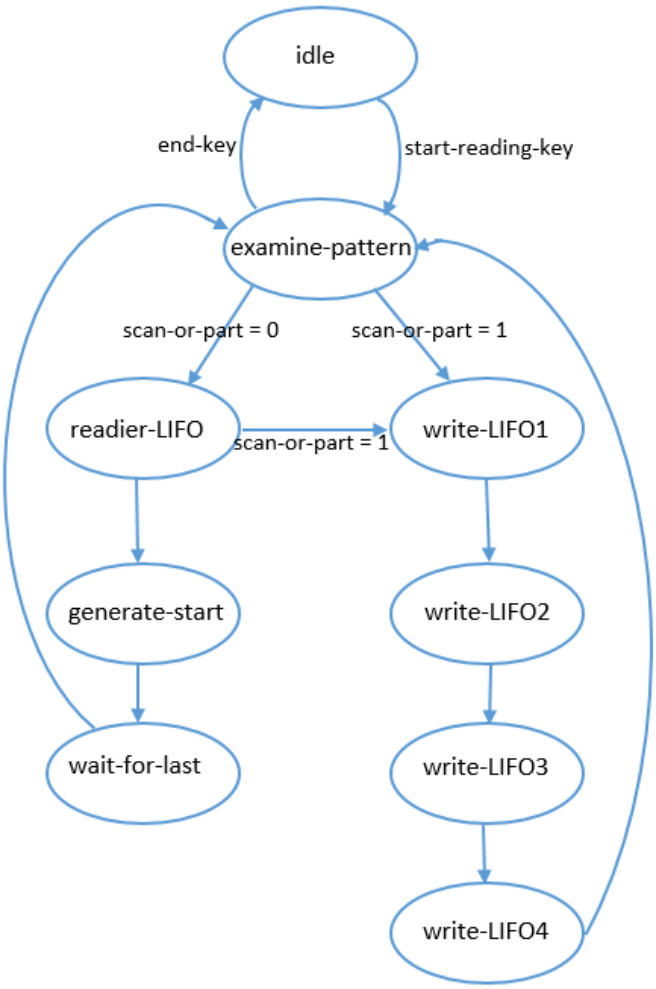
4

13- مسح المربع ذو الرقم (4).

LIFO

Empty

من أجل إنجاز المهمة السابقة، نستخدم آلة الحالة التي تظهر في الشكل (7.5).



الشكل (7.5) مخطط آلة الحالة للمتحكم FSM.

نقوم في الحالة Ezmine-pattern بفحص المخطط الحالي، فإذا كان مخطط تقسيم نقوم بكتابة عناوين رؤوس المربعات الجزئية الأربعة الموافقة للتقسيم، وإذا كان مخطط مسح أوليّ نقوم بقراءة رأس المربع المطلوب، وإعطاء أمر المسح خلال الحالة Generate-start، ثمّ ننتظر نهاية مسح المربع الجزئي في الحالة wait-for-last، عند انتهاء المسح نعود إلى الحالة Examine-pattern، لاستكمال قراءة المفتاح.

تقوم وحدة التحكم بإعطاء نوع المسح، رقم تحويله، حجم المربع الجزئي وعنوان رأس المربع الجزئي {jst, ist} إلى وحدة المسح Scan، التي تحتوي عنصراً مولّداً لكل نوع من أنواع المسح، ويكون خرج هذه الوحدة عنوان المسح rdaddr-out = {jcurrent, icurrent}.

كما تقوم وحدة التحكم بإعطاء نوع التقسيم، رقم تحويله، حجم المربع الجزئي وعنوان رأس المربع الجزئي {jst, ist} إلى وحدة التقسيم، التي تقوم بحساب عناوين رؤوس المربعات الجزئية الجديدة الناتجة عن التقسيم، بحسب الترتيب المحدد برقم التحويل، وهي: {j0, i0}, {j1, i1}, {j2, i2}, {j3, i3}.

2.6.5- وحدة تبديل قيم البيكسلات الخاصة بالتعمية Enc unit

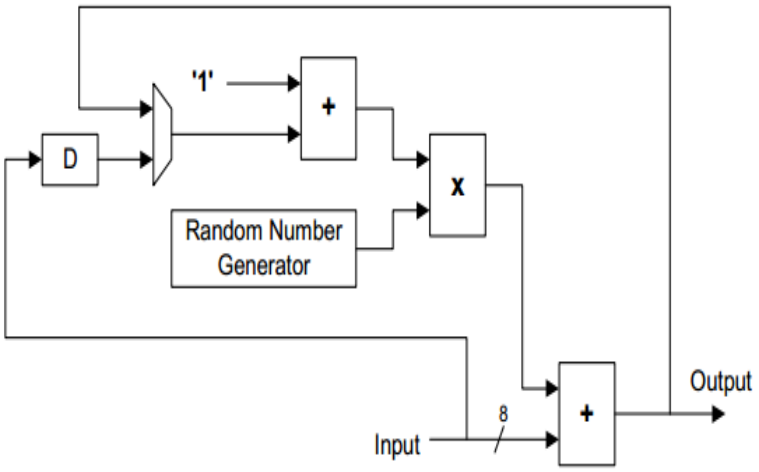
تهدف هذه الوحدة إلى تحقيق خاصتي النثر والخلط على الصورة المعمّاة، حيث تقوم بإضافة أعداد عشوائية إلى قيم بيكسلات الصورة الواضحة، وتنتج هذه الأعداد عن وحدة توليد الأعداد العشوائية التي سنأتي على شرحها لاحقاً.

يجري عند التعمية استخدام العلاقة التالية لتبديل قيم بيكسلات [11].

$$C[0] = B[0]$$
$$C[j] = \big(B[j] + \big((C[j-1]+1) * R[j]\big) mod 256\big) mod 256 \quad j > 0$$

يمثل العدد j ترتيب البيكسل.

جرى تصميم هذه العلاقة باستخدام جامعين وضارب، كما يظهر الشكل (8.5).



الشكل (8.5) وحدة تبديل قيم البيكسلات في التعمية.

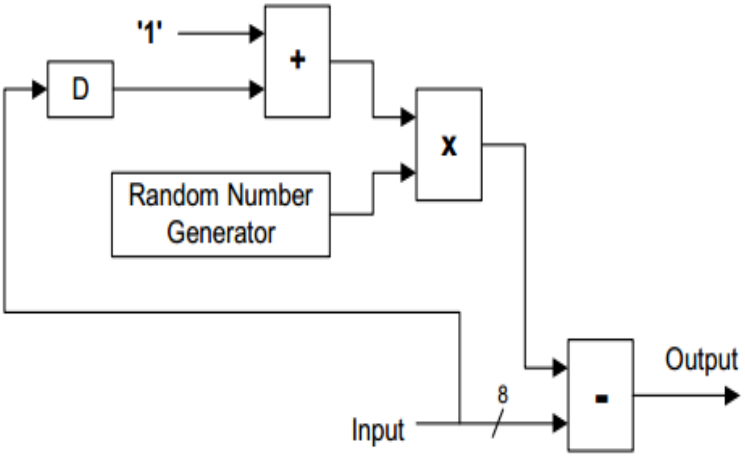
ويجري الحصول على تابع القسمة (mod) بأخذ البتات الثمانية الأولى من نتيجة الضرب أوالجمع.

3.6.5- وحدة تبديل قيم البيكسلات الخاصة بفك التعمية DEC unit

من أجل استرجاع قيم بيكسلات الصورة الأصلية، يجري استخدام العلاقة التالية [5]:

$$B[0] = C[0]$$
$$B[j] = \big(C[j] - \big((B[j-1]+1) * R[j]\big) mod 256\big) mod 256 \quad j > 0$$

جرى تصميم هذه العلاقة باستخدام جامع وضارب وطارحكما يوضح الشكل (9.5).



الشكل (9.5) وحدة تبديل قيم البيكسلات في فك التعمية.

4.6.5- مولّد الأعداد العشوائية

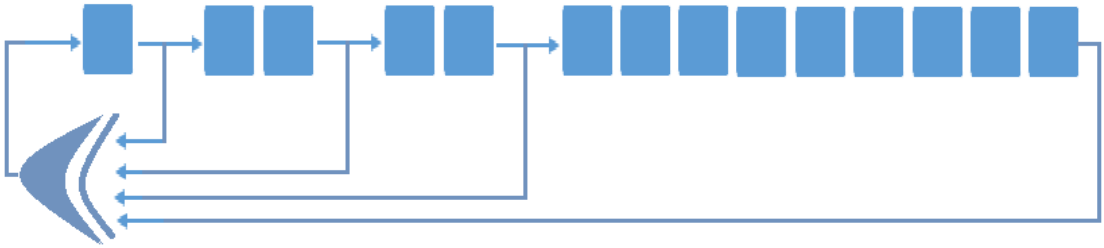
يتألف مولّد الأعداد العشوائية من سجلات إزاحة ذات تغذية خلفية خطية (Linear Feedback Shift Registers (LFSRs))، يرتبط كل مولد بكثير حدود مميّز له، رتبته تعادل طول سجل الإزاحة، وقيمته تحدد طريقة التغذية الخلفية.

وللحصول على ثمانية بتات عشوائية، جرى اختيار ثمانية مولدات عشوائية تختلف عن بعضها بكثير الحدود المميز لكلّ منها، وبحيث يعطي كل سجل بت واحد. وكثيرات الحدود التي جرى اختيارها هي:

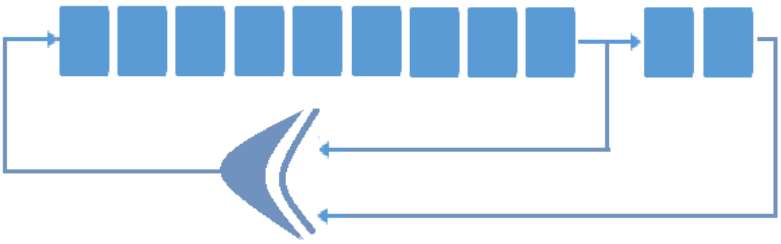
$$f_1(x) = x^{14} + x^5 + x^3 + x + 1$$
$$f_2(x) = x^{11} + x^9 + 1$$
$$f_3(x) = x^9 + x^5 + 1$$
$$f_4(x) = x^{12} + x^6 + x^4 + x + 1$$
$$f_5(x) = x^{13} + x^4 + x^3 + x + 1$$
$$f_6(x) = x^8 + x^6 + x^5 + x^4 + 1$$
$$f_7(x) = x^{10} + x^7 + 1$$
$$f_8(x) = x^7 + x^6 + 1$$

تكون أطوال سجلات الإزاحة 14، 11، 9، 12، 13، 8، 10، 7، على الترتيب. يجب أن لا ينعدم خرج سجلات الإزاحة ، ولذلك كما هو ملاحظ جرى اختيار كثيرات الحدود بحيث لا ينعدم الحد الثابت. يوضح

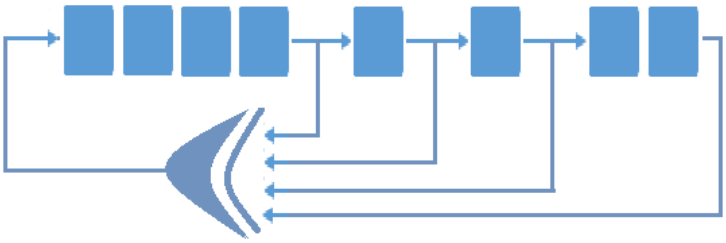
الشكل (10.5) بعض مولدات الأرقام العشوائية المستخدمة، حيث يظهر استخدام بوابة من نوع XOR، من أجل تحقيق التغذية الخلفية. تتألف مداخل هذه البوابة من مخارج السجلات المتوافقة مع أسس كثير الحدود المميز. ويكون مخرج هذه البوابة دخلاً للسجل الأول.



$$f_1(x) = x^{14} + x^5 + x^3 + x + 1$$



$$f_2(x) = x^{11} + x^9 + 1$$

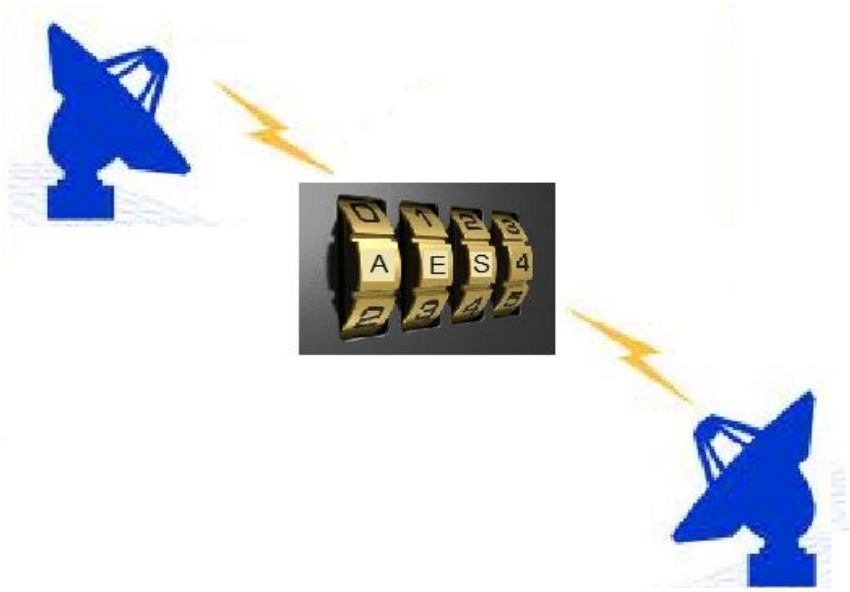


$$f_6(x) = x^8 + x^6 + x^5 + x^4 + 1$$

الشكل (10.5) سجلات الإزاحة الخاصة ببعض بتات مولد الأعداد العشوائية.

الفصل السادس

اختبار أداء نظام الاتصال المعمّى باستخدام خوارزمية المسح SCAN



يقدّم هذا الفصل نتائج الاختبارات التي قمنا بها على بطاقة DE2_115، حيث جرى اختبار خوارزمية التعمية، بجزأيها التعمية وفك التعمية، وذلك من خلال تعمية العديد من الصور والفيديو، وفك تعميتها، ومقارنتها مع نتائج عملية المحاكاة باستخدام MATLAB.

1.6- إختبار خوارزمية المسح SCAN

أجرينا اختبارات متعددة لخوارزمية المسح SCAN، وذلك للتصميمين الذين جرى توضيعهما على شريحة FPGA:

- ⇦ التصميم الأول يختص بتعمية الصور.
- ⇦ التصميم الثاني، ويختص بتعمية المعطياة الفيديوية والتلفزية، حيث جرى استخدام كاميرا، وجرت التعمية بالزمن الحقيقي.

جرى اتّباع عدة سيناريوهات للتأكد من صحّة نتائج التعمية:

1.1.6- السيناريو الأول

جرى مسح العديد من الصور بمخططات المسح المعمّمة (تعميتها بدون مرحلة الإضافة العشوائية)، وتم التأكد من صحة المسح، وذلك طبعاً بالمقارنة مع المحاكاة ضمن MATLAB. يُظهر الشكل (1.6) مثال عن مسح صورة وذلك باستخدام مخطط مسح معمّم بسيط، مكّون من مخطط تقسيم واحد ومخطط مسح أوليّ واحد مكرر أربع مرات، من أجل المصفوفات الأربعة الناتجة عن مخطط التقسيم.

-الصورة المعمّاة- -الصورة الواضحة-

الشكل (1.6) مثال عن مسح صورة بدون مرحلة إضافة القيم العشوائية.

2.1.6- السيناريو الثاني

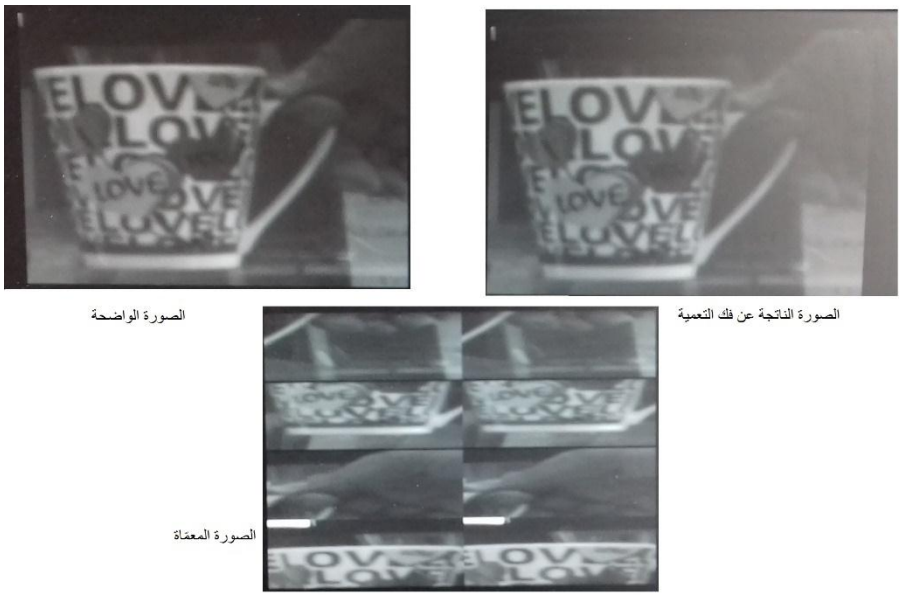
جرى مسح العديد من الصور بمخطط المسح المعمّم، بالإضافة إلى مرحلة إضافة القيم العشوائية، وتم التأكد من صحة المسح، وذلك بإعادة الصورة الأصلية بعملية فك التعمية، ثمّ بالمقارنة مع الصورة الأصلية. يُظهر الشكل (2.6) مثال عن تعمية صورة وذلك باستخدام خوارزمية المسح، باستخدام التصميم الأول المخصص لتعمية الصور، وجرت عملية فك التعمية، ثم كتابة الصورة الناتجة في الذاكرة التي تحوي الصورة الأصلية، وإظهارها على الشاشة.

-الصورة المعمّاة- -الصورة الواضحة-

الشكل (2.6) مثال عن تعمية صورة باستخدام خوارزمية المسح.

3.1.6- السيناريو الثالث

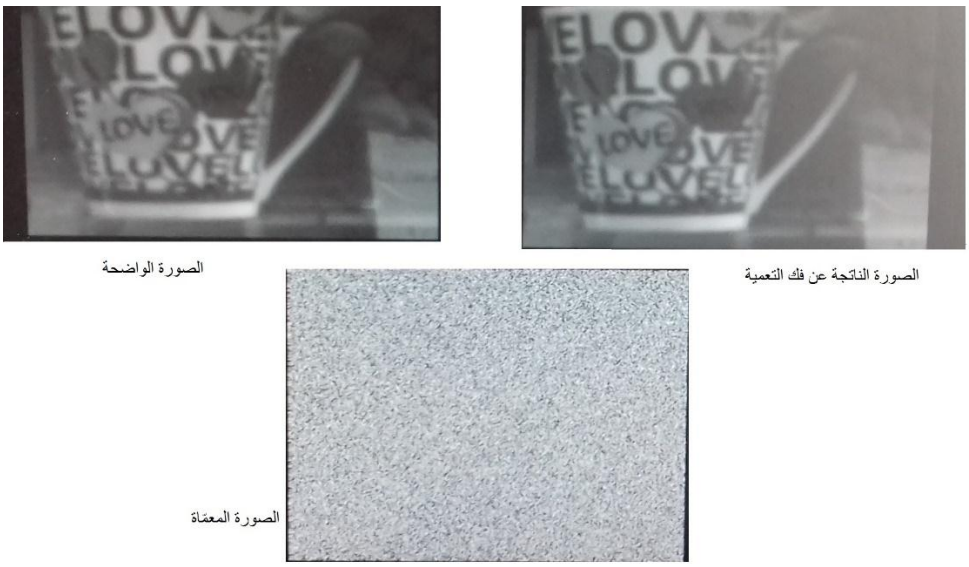
جرى استخدام التصميم الثاني المخصص لتعمية المعطيات التلفزية والفيديوية، بالإضافة إلى استخدام الكاميرا الرقمية TRDB_D5M، وجرت عملية التعمية باستخدام خوارزمية المسح، لكن دون مرحلة الإضافة العشوائية، ثم جرت عملية فك التعمية، وعُرض كلّ من الفيديو الأصلي، المعمّى والمستعاد بعملية فك التعمية على الشاشة. يُظهر الشكل (3.6) لقطة للشاشة عند تعمية مقطع الفيديو المأخوذ من الكاميرا، بدون مرحلة الإضافة العشوائية.



الشكل (3.6) لقطة للشاشة عند تعمية معطيات الكاميرا، بدون إضافة العشوائية.

4.1.6- السيناريو الرابع

جرى استخدام التصميم الثاني المخصص لتعمية المعطيات التلفزية والفيديوية، بالإضافة إلى الكاميرا الرقمية TRDB_D5M، وجرت كما في السيناريو السابق عملية التعمية باستخدام خوارزمية المسح، ثم جرت عملية فك التعمية، يُظهر الشكل (4.6) لقطة للشاشة عند تعمية مقطع الفيديو المأخوذ من الكاميرا، مع مرحلة إضافة العشوائية.



الشكل (4.6) لقطة للشاشة عند تعمية معطيات الكاميرا، مع إضافة العشوائية.

2.6- الكلفة العتادية لكلّ من التصميمين

بعد تصميم خوارزمية المسح SCAN، قمنا بتحميل النظام على بطاقة التطوير DE2-115، وذلك لكل من التصميمين، التصميم المخصص لمسح الصور، والتصميم المخصص لتعمية الفيديو، ووجدنا أنه لم يستهلك إلا جزءاً صغيراً جداً من العتاد الصلب الذي تتيحه هذه البطاقة. والجدول (1.6) يوضح تقرير العتاد الصلب الذي يستهلكه النظام، ويعطي مقارنة بين التصميمين.

نوع العتاد الصلب	كلفة التصميم الأول (المخصص لمسح الصور)	كلفة التصميم الثاني (المخصص لمسح الفيديو)
Total logic elements	8,680/114,480 (8%)	9,600/114,480 (8%)
Total combinational functions	7,478/114,480 (7%)	8, 072/114,480 (7%)
Dedicated logic registers	3,475/114,480 (3%)	4,492/114,480 (4%)
Total pins	78 /529 (15%)	428 /529 (81%)
Total memory bits	1,572,864 /3.981.312 (41%)	1,622,072 /3.981.312 (41%)
Embedded Multiplier 9-bit elements	2/532 (<1%)	2/532 (<1%)
Total PLLs	0/4 (0%)	1/4 (25%)

الجدول (1.6) الكلفة العتادية اللازمة لتنفيذ خوارزمية المسح SCAN.

نلاحظ من الجدول (1.6) أنّ التصميمين لا يستهلكان قدراً كبيراً من العناصر المنطقية (LE: Logic Elements). فإنّ كلً من التصميمين يستهلك 8% من العناصر المنطقية التي تحويها الشريحة فقط، كما نلاحظ أنه يوجد استهلاك قليل جداً للضوارب في التصميمين، وذلك لأنه توجد عمليتي ضرب فقط، في مرحلة إضافة العشوائية، واحدة عند التعمية، والثانية عند فك التعمية. كما يجري استخدام عدد من PLLs من أجل تقسيم الساعة. يجري استهلاك نفس القدر من الذواكر، لأنه في مرحلة تعمية الفيديو، لايتم تخزين ملف

الفيديو، وإنما يتم الحصول عليه من الكاميرا الرقمية، ثم يجري تعميته مباشرةً (بالزمن الحقيقي)، وعرضه مباشرةً على الشاشة.

الفصل السابع

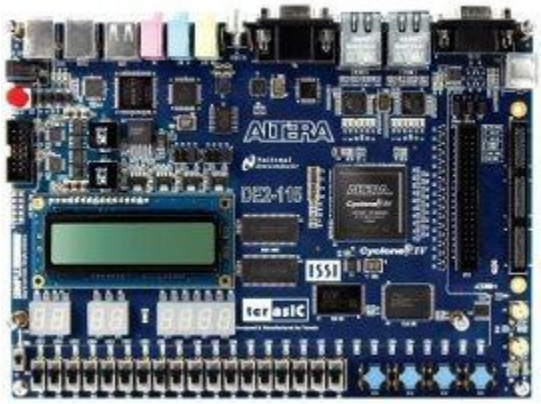
الخاتمة والآفاق المستقبلية

يعرض هذا الفصل الأدوات التي تمّ استخدامها في تصميم وتنفيذ نظام الاتصال المعمّى، سواء العتادات Hardware، أو البيئات البرمجية Software. كما يعرض المشاكل والصعوبات التي واجهت بناء النظام، والحلول التي تمّ اعتمادها لحل المشاكل وتذليل الصعوبات. ثمّ يعرض خاتمة العمل والنظام الذي نتج في نهاية المشروع، وأخيراً يعرض الآفاق المستقبلية للنظام.

1.7- الأدوات المستخدمة في إنشاء نظام الاتصال المعمّى

استخدمنا في بناء نظام الاتصال المعمّى عتاديات Hardware، مبيّناً في الشكل (1.7)، وتتمثّل بما يلي:

- شريحة FPGA واحدة تمثّل المعمّي ومفكك التعمية بآن واحد، على بطاقة تطوير من النوع Altera DE2-115.



الشكل (1.7) العتاد الصلب المستخدم في نظام الاتصال المعمّى.

كما استخدمنا عدة بيئات برمجية Software، لإنجاز المحاكاة و تعريف الكيان الصلب، وهي:

- بيئة MATLAB R2015a، واستخدمناه لإجراء محاكاة كل من خوارزميتي التعمية المعيارية AES، والمسح SCAN، وتنفيذ اختبارات الأداء لكلّ من الخوارزميتين.
- بيئة Quartus II، لغة توصيف الكيان الصلب VHDL، لتوصيف الكيان الصلب الذي يقوم بتنفيذ مراحل خوارزمية المسح SCAN.
- بيئة ModelSim، وتستخدم من أجل محاكاة التصميم عن طريق إظهار إشارات المداخل، المخارج والإشارات البينية للتصمي، والتحقق من صحّة عمل الخوارزمية وتحقق التزامن.

2.7- المشاكل والصعوبات

واجهنا في هذا العمل العديد من التحديات والصعوبات، بحيث تمكنّا من حلّ بعض المشاكل.

- صعوبة الحصول على توصيف دقيق لمخططات المسح الأولية، حيث جرى دراستها بعناية، ثم جرى بناء توابع تقوم بتوليد عناوين موافقة لها في MATLAB، وجرى توصيف كيان صلب لها باستخدام اللغة VHDL.
- طول وتعقيد الرماز الخاص بتوصيف الكيان الصلب باستخدام اللغة VHDL: من التحديات التي تمكنّا من التغلّب عليها.

3.7- الخاتمة

جرى في هذا المشروع ما يلي:

- تنفيذ محاكاة عمل خوارزمية التعمية باستخدام مخططات المسح SCAN ضمن بيئة MATLAB.
- تنفيذ محاكاة لاختبارات العشوائية التي تقييّم أداء خوارزميات التعمية ضمن بيئة MATLAB.
- إخضاع كلّ من خوارزمية التعمية المعيارية AES وخوارزمية المسح SCAN إلى اختبارات العشوائية، ومقارنة النتائج، ونتج عن هذه المقارنة التأكد من فعالية خوارزمية المسح وصلاحيتها في تقديم الأمان المطلوب والسرعة اللازمة للعمل بالزمن الحقيقي.
- توصيف الكيان الصلب اللازم لمعمّي ولمفكّك تعمية خوارزمية المسح SCAN ، باستخدام لغة توصيف الكيان الصلب VHDL.
- التأكد من عمل خوارزمية التعمية السابقة بالعديد من التجارب والإختبارات.

4.7- الآفاق المستقبلية

من الآفاق المستقبلية، التي يمكن أن تحسّن عمل خوارزمية المسح SCAN وفعاليتها في التعمية وفي العمل بالزمن الحقيقي:

- زيادة عدد مخططات المسح الأولية الموصفة بلغة توصيف الكيان الصلب VHDL، وينتج عن ذلك زيادة في عدد مفتايح التعمية المتاحة، مما يزيد من الأمان الذي تقدمه خوارزمية المسح.
- زيادة سرعة معالجة عمليتي التعمية وفك التعمية باستخدام Pipelining، وذلك بزيادة العتاد الصلب المخصص لهاتين العمليتين. ويؤدي ذلك إلى تحسين العمل بالزمن الحقيقي.

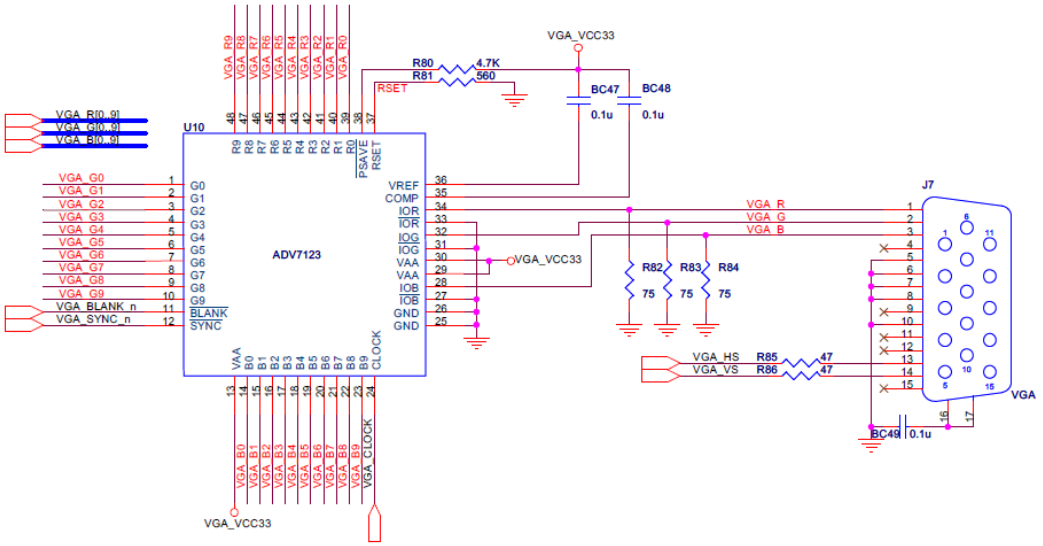
ومن الآفاق المستقبلية، استخدام خوارزمية المسح في قناة اتصال، في شبكة آمنة متكاملة، لنقل معطيات فيديوية أو صورية سرية تخص مؤسسة تجارية أو مدنية أو شخصية.

الملاحق

الملحق A

وحدة الإظهار VGA

- ⇦ تعتمد على الشريحة ADV7123 التي تمثّل محول رقمي_تماثلي يتمتع بالمواصفات التالية: triple 10-bit high-speed video DAC, 140 MHz.
- ⇦ دقة تصل إلى 1600 x 1200.
- ⇦ يمكن استعماله لبناء مرمِّز التلفاز (TV encoder) ذو الأداء العالي.
- ⇦ الشكل (1.A) يبيّن مخطط دارة VGA.



الشكل (1.A) مخطط دارة VGA.

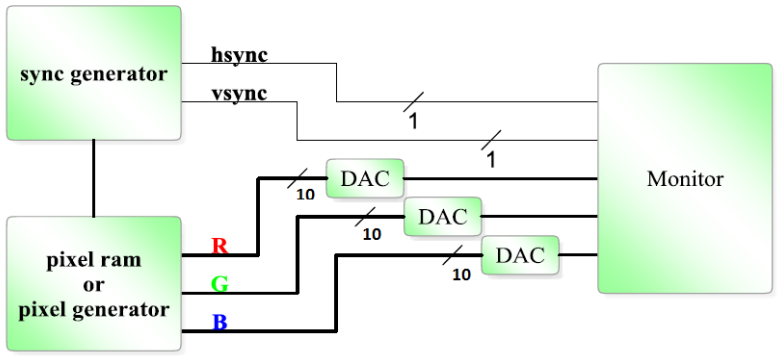
- ⇦ نظام VGA يتألف من خمس إشارات، هذه الإشارات موضّحة في الجدول (1.A).

اسم الإشارة	التوصيف
hsync	إشارة التزامن الأفقي
vsync	إشارة التزامن العامودي

red	التمثيل الرقمي لمستوى اللون الأحمر في نظام RGB (10-bits)
green	التمثيل الرقمي لمستوى اللون الأخضر في نظام RGB (10-bits)
blue	التمثيل الرقمي لمستوى اللون الأزرق في نظام RGB (10-bits)

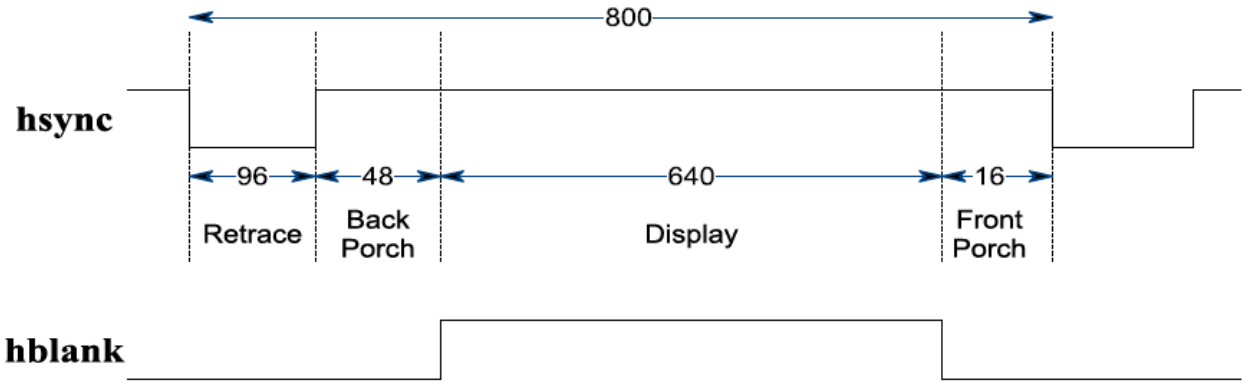
الجدول (1.A) توصيف إشارات VGA.

وهذه الإشارات مبيّنة في المخطط الصندوقي في الشكل (2.A).



الشكل (2.A) مخطط VGA الصندوقي.

⇦ يوضّح الشكل (3.A) إشارات التزامن الأفقي من أجل العرض على شاشة VGA.



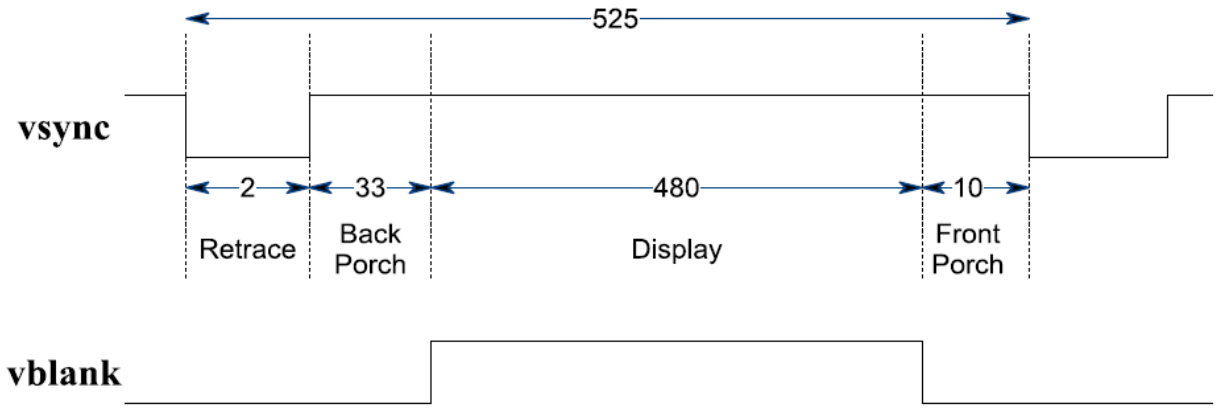
الشكل (3.A) التزامن الأفقي لنظام VGA.

نستطيع أن نلاحظ أن دور كامل من إشارة المزامنة الأفقية (hsync) تتضمن 800 بيكسل (سطر واحد) و هي مقسمة إلى أربع مجالات كما هو موضح في الجدول (2.A).

اسم المجال	عدد نقاط الشاشة (#Pixels)	التوصيف
Back Porch	16	إشارة الفيديو غير مؤثرة أثناء هذه الفترةِ
Display	640	مجال عرض المعطيات. تقود بيانات نظام RGB تباعاً كل نقطة بالشاشة عبر السطر الجاري عرضه.(المنطقة المرئية من الشاشة)
Front Porch	48	إشارة الفيديو غير مؤثرة أثناء هذه الفترةِ
Retrace	96	تحدد نهاية سطر المعطيات و بداية السطر التالي

الجدول (2.A) توصيف إشارات التزامن الأفقي في نظام VGA.

⇦ إن إشارة التزامن العامودي (vsync) شبيهة بإشارة التزامن الأفقي، عدا أنّ النبضة الأولى تبين نهاية إطار Frame وبداية آخر. كما هو موضّح في الشكل (4.A).



الشكل (4.A) مواصفات التزامن العامودية لنظام VGA.

References

[1] Roshni Padate, Aamna Patel. “Image encryption and decryption using AES algorithm”, INTERNATIONAL JOURNAL OF ELECTRONICS AND COMMUNICATION NGINEERING & TEcHNOLOGY (IJECET), 2015.

[2] M.A. Murillo-Escoba, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez, O.R. Acosta Del Campo. “A RGB image encryption algorithm based on total plain image characteristics and chaos”, ScienceDirect, Signal Processing , Volume 109, April 2015, Pages 119–131.

[3] Yuanmei Wang, Tao Li. “Study on Image Encryption Algorithm Based on Arnold Transformation and Chaotic System”, IEEE, Intelligent System Design and Engineering Application (ISDEA), 2011.

[4] BRUCESCHNEIER, "APPLIED CRYPTOGRAPHY", SECOND EDITION, ترجمة: د. حاتم النجدي، د. أميمة الدكاك، "التعمية التطبيقية"، من مطبوعات الجمعية العلمية السورية للمعلوماتية، 2006.

[5] A. Dollas N. Bourbakis and C. Kachir. "Performance analysis of fixed, reconfigurable, and custom architectures for the scan image and video encryption algorithm". IEEE, Field Programmable Custom Computing Machines (FFCM), 2003.

[6] Federal Information Processing Standards Publication 197 (FIPS PUBS) of National Institute of Standards and Technology (NIST). Announcing the advanced encryption standard (aes), 2001.

[7] S. Agaian Y. Wu, J. P. Noonan. "NPCR and UACI randomness tests for image encryption". Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011.

[8] Dr V. Jaglan V. Thada, Dr. K.N.M. Compa-rison of jaccard, dice, cosine similarity coefficient to find best fitness value for web retrieved documents using genetic algorithm. International Journal of Innovations in Engineering and Technology (IJIET), 2013.

[9] DE2-115, Devlopment and Education Bord, User Manual, Copyright © 2003-2010 Terasic Technologies Inc.

[10] TRDB-D5M, 5 Mega Pixel Digital Camera Devlopment Kit, User Manual, Copyright © 2003-2010 Terasic Technologies Inc.

[11] C. Kachir, A. Dollas, D. Pnevmatikatos and K. Kalaitzakis. "Design and FPGA Implementation of the SCAN Encryption Algorithm", Technical University of Crete, Department of Electronic and Computer Engineering, Chania-Greece, 2003.

[12] C. Shannon. “Communication theory of secrecy systems”, Bell Systems Technical Journal 28, 656 – 715, 1949.

[13] L. Tag, “For Encrypting and Decrypting MPEG Video Data Efficiently”, in Proceeding of the Firth ACM International Multimedia Conference, 1996, pp. 219-230.

[14] C. Shi and B. Bhargava,” Light Weight MPEG video Encryption Algorithm”, in Proceeding of the International Conference on Multimedia, 1998, pp. 55-61.

[15] J. meyer and F. Gadegast," Security Mechanisms for Multimedia Data with the Example MPEG-1 video", Project Description of SECMPEG, Technical University of Berlin, 1995.