جامعة الموصل

كلية الهندسة

تحقيق التشفير H.264/AVC على مصفوفة البوابات المنطقية المبرمجة حقلياً وتمثيل التشفير وفك التشفير باستخدام Matlab

رسالة تقدمت بها

نـــــور نـــــواف حمـــــدون الصـــــواف

إلى

مجلس كلية الهندسة في جامعة الموصل وهي جزء من متطلبات نيل شهادة

الماجستير في الهندسة الكهربائية/اتصالات وإلكترونيك(إلكترونيك)

بإشراف

الدكـــتور محمـــــد حـــــازم الجمـــــاس

جمادي الأول/1438هـ

آذار/2017

Abstract

Hybrid encryption standard H264/AVC is one of the strongest and the latest advanced encryption standard and data processing used in modern data compression systems, for its strength and flexibility in video data encryption .

Single data compression and encryption system works on encryption and decryption for display of various types of data. The objective of the dissertation is to implement all the encryption and cryptographic components by MATLAB program and representation of my work on a chip FPGA .

The design has been applied to images and videos in diffrent sizes starting from QCIF TO HD. The dissertation contained two parts characterized by implementing all the encryption components using simulation MATLAB. A single discrite cosine transform function(1D-DCT) has been appled and compared with two dimensional discrite cosine transform function and data retrieved .Then apply this function on the video with encryption items.

The video size is (90KB) and (164.2 MB) .Affter appling the compration algorithm the becames size(45KB) and (82.1MB) with dimensions frame size(288x352) and (250x320) were obtained respectively and the image quality (PSNR) obtainted is equal (38.78db) and (73.8db) . The first algorithm includes intra frame(I-Frame) and used second mode is the called (DC Mode). The encryption time for intra frame is(0.099s) and The decryption time (0.000317s) . The second algorithm includes two dimensional logarithm search (2D-logarithem search) is predication frame (Inter-frame(P)).The encryption time is equle (0.00342s) and decryption time is equal (0.00011s). The encryption and decryption time frame is (2.979s) of intra frame, but the time of encryption and decryption for intre frame is (0.1059s) of period video(30fps).

The second part of the dissertation represents the implementation of encryption and decryption by using FPGA .The Intra frame(I-frame) time is (2.77ms) with size frame (288x352). The time is (83.1ms) within (30fps) and the number of the slices (3714). The all Components (integer conversion function, and the rounding function, the inverse transfer function, the inverse function approximation), an area of 92% of total chip size during execution on chip within 68MHZ frequency within Programmed of practical applications with version 14.1 and company on a chip Spartan3E(XC3S500E).

The aim of the practical representation can be summarized by the time difference between working with simulation for the MATLAB program and practical design on FPGA, so the total time to encrypt and decrypt. The first frame in the program MATLAB is that (2979.51ms) While the practical investigation on FPGA is (83.1 ms) within (30fps).

University of Mosul

College Engineering

FPGA Implementation of H.264/AVC Encoder and MatLab Simulation of H.264/AVC Encoder/Decoder

presented by the

Noor Nawaf Hamadoun Al-Sawaf

To

Board of the Faculty of Engineering at the University of Mosul as part of the certification requirements

Master's degree in electrical engineering / communications and electronic (electronic)

supervision of

Dr. Mohammed Hazem A-ljmmas

2017 1438H

المستخلص بلغة الرسالة

يعدَ معيار التشفير الهجين H264/AVC من أقوى وأحدث معايير التشفير المتقدم في التشفير ومعالجة البيانات المستخدم في أنظمة ضغط البيانات الحديثة, وذلك لما يمتلكه من قوة ومرونة في التشفير البيانات الفيديوية والصورية المطلوب نقلها.

نظام التشفير وضغط البيانات الأحادي يعمل على التشفير وفك التشفير للبيانات الصورية بأنواعها المختلفة, وكان هدف الرسالة هو تنفيذ جميع مكونات التشفير وفاتح التشفير بمحاكاة ألMATLAB وتمثيل عملي على رقاقة FPGA لجميع البيانات ذات الأحجام الصغيرة والكبيرة كما في حالة الصور الرمادية والصور الملونة وملفات الفيديو مع المحافظة على مستوى عالٍ من الجودة في عملية الاسترجاع. وتم تطبيق التصميم على صور والفيديو بجميع الأحجام ابتداءً منQFC إلىHD. وتضمنت الرسالة جزأين متمثلة بتنفيذ جميع مكونات التشفير بإستعمال محاكاة MATLAB(2013Ra)وبصورة تدريجية تم الوصول إلى الهدف الرئيس ابتداءً من كيفية التعامل مع الصور المفردة وتطبيق دالة تحويل الجيب تمام الأحادية (1D−DCT) ومقارنتها مع دالة تحويل الجيب تمام الثنائية (2D-DCT) واسترجاع البيانات ومن ثم تطبيق هذه الدالة على الفيديو مع إدخال عناصر التشفير.

وكان العمل على فيديو بحجم (90kB) (164.2MB) وعن طريق تنفيذ نوعين من الخوارزميات تم الحصول على حجم (45kB) و(82.1MB) أبعاد اطار(288X352) و(250X320) على التوالي وبجودة صورة (PSNR) تساوي(38.78db) و(37.8db) في (30fps). تتضمن الخوارزمية الأولى تشفير الإطار البيني (Intra frame) وتتمثل بتطبيق النمط الثاني من الخوارزمية المسمى (DC mode) حصلنا على زمن التشفير(0.099s) وزمن فك التشفير (0.000317s) والخوارزمية الثانية هي خوارزمية البحث اللوغاريتم ثنائي الأبعاد (2D-logarithem search) الخاصة لتشفير الإطارات الحركية (Inter frame) وحصلنا على زمن التشفير(0.00342s) وزمن فك التشفير(0.00011s) لحجم الصورة نفسه , ان زمن تشفير وفك تشفير الاطار البيني هو (2.979s) وزمن تشفير وفك تشفير الاطار الحركي هو(0.1059s) لفيديو(30fps) .

أمَا الجزء الثاني من الرسالة فتمثل بتنفيذ التشفير وفك التشفير لخوارزمية الإطار البيني ضمن زمن (2.77 ms) لحجم إطار(288x352) أي (83.1ms) في حال استخدام فيديو (30fps) واستهلاك ما يقارب (3714) من الشرائح لتنفيذ جميع مكونات التشفير(دالة تحويل الأعداد الصحيحة , ودالة التقريب , معكوس دالة التحويل , ومعكوس دالة التقريب) أي بمساحة 92% من حجم الرقاقة الكلية اثناء التنفيذ على الرقاقة ضمن حدود تردد 68MHZ ضمن برنامج التطبيقات العملية ISE ذات الإصدار 14.1 الخاص بشركة Xilinx وعلى رقاقة Spartan3E(XC3S500E).

ان الغاية من تمثيل العملي يمكننا تلخيصها بالفرق الزمني مابين العمل باستخدام المحاكاة للبرنامج ال(matlab) والتصميم العملي, حيث الزمن الكلي لتشفير الاطار الاول وفك تشفيره في المحاكاة لبرنامج (matlab) يتمثل (2979.51ms) بينما في التحقيق العملي يتمثل(83.1 ms) لكل (30fps).

د. عمر موفق محمود اليوسف
معاون العميد للشؤون العلمية والدراسات العليا