A Format-Compliant Selective Encryption Scheme for Real-Time Video Streaming of the H.264/AVC

Fatma SBIAA
University of South Brittany
Laboratory of Information Science and Technology, communication and Knowledge (Lab-STICC)
Lorient, France

Medien ZEGHID
University of Monastir
Laboratory of Electronics and Microelectronics
Faculty of Sciences
Monastir, Tunisia

Mohsen MACHHOUT
University of Monastir
Laboratory of Electronics and Microelectronics
Faculty of Sciences
Monastir, Tunisia

Sonia KOTEL
Department of Informatics
Higher Institute of Computer Science and Communication Techniques of Hammam Sousse
Hammam Sousse, Tunisia

Rached TOURKI
University of Monastir
Laboratory of Electronics and Microelectronics
Faculty of Sciences
Monastir, Tunisia

Adel BAGANNE
University of South Brittany
Laboratory of Information Science and Technology, communication and Knowledge (Lab-STICC)
Lorient, France

***Abstract*—H.264 video coding standard is one of the most promising techniques for the future video communications. In fact, it supports a broad range of applications. Accordingly, with the continuous promotion of multimedia services, H.264 has been widely used in real-world applications. A major concern in the design of H.264 encryption algorithms is how to achieve a sufficiently high security level, while maintaining the efficiency of the underlying compression process. In this paper a new selective encryption scheme for the H.264 standard is presented. The aim of this work is to study the security of the H.264 standard in order to propose the appropriate design of a hardware crypto-processor based on a stream cipher algorithm. Since the proposed cryptosystem is mainly dedicated to the multimedia applications, it provides multiple security levels in order to satisfy the requirements of various applications for different purposes while ensuring higher coding efficiency. Different performance analyses were made in order to evaluate the new encryption system. The experimental results showed the reliability and the robustness of the proposed technique.**

***Keywords*—component; Video coding; Data encryption; Data compression; H.264/AVC**

I. INTRODUCTION

Different multimedia applications have become increasingly popular due to the fast development of communication technologies. Since communications across public networks can easily be intercepted, privacy becomes a major concern for commercial uses of multimedia communication. Encryption is an important tool for providing the security services in different fields of applications. Thus, since the 1990s, many research efforts have been devoted to the development of certain video encryption algorithms. Therefore, many algorithms have been proposed to ensure the confidentiality of video data.

Multimedia data requires either full encryption or selective encryption depending on the application requirements [1]. For example military and law enforcement applications require full encryption. However, there is a large spectrum of applications that demands a lower security level. These applications require the development of a cryptosystem using a selective encryption.

To clearly identify the characteristics of video encryption algorithms, the encryption algorithms can be divided according to their association (or not) with the video compression process. We distinguish the encryption algorithms joint compression and others independent of the compression. In fact, there are three different approaches which combine encryption and compression. As shown in “Fig. 1”, an encryption algorithm could be placed before, during, or after the compression process [2][3].

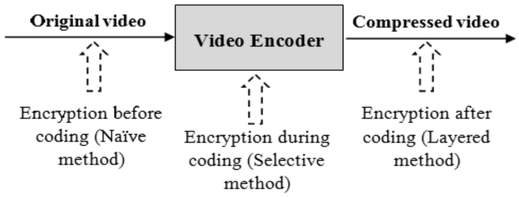

Original video
Video Encoder
Compressed video
Encryption before coding (Naïve method)
Encryption during coding (Selective method)
Encryption after coding (Layered method)

Fig. 1. Video Encryption Techniques

The video encryption algorithms placed before or after compression are called encryption algorithms independent of the compression while those executed during the compression process are called encryption algorithms joint compression.

The direct approach consists in the encryption of the entire compressed video stream using a conventional cryptographic method, such as the Advanced Encryption Standard (AES). This approach is called the naive approach. However, conventional cryptographic algorithms, which are generally designed to encrypt text data, are not well suited for video encryption because they can’t treat the large volume of video data in real time. In addition, it is almost impossible to adapt them to specific paradigms of video applications which pose specific requirements that are never encountered during the encryption of text data. These requirements are related to the efficiency of encryption, the security needs, the code conformity of the video stream, the compression efficiency, the respect for the syntax and the perception. They can be ensured using the selective encryption. In fact, this kind of encryption treats a part of the plaintext and presents two main advantages. First, it reduces the computational requirements, since only a part of plain-data is encrypted. Second, encrypted bitstream maintains the essential properties of the original bitstream. It just prevents abuse of the data. In the context of video encryption, it refers to destroying the commercial value of the video stream to a degree which prevents a satisfying viewing capability. The H.264/AVC-based selective encryption schemes have been already presented on CAVLC and CABAC [3]. These two previous methods fulfill real-time constraints by keeping the same bitrate and by generating completely compliant bitstream.

This paper presents a new selective encryption method for the H.264/AVC videos. The second section is devoted to introduce the H.264/AVC standard and the related encryption schemes. The third section will discuss the system specification, the choice of algorithms and the cryptographic techniques (scenarios). The fourth section is devoted to the design and the implementation of proposed cryptosystem. The next step is the Hardware/software validation on FPGA platform taking into account the real-time aspect.

II. H.264/AVC –Based Video Encryption

In this section, we will present the H.264/AVC video coding as well as its bit stream syntax structure. Then, we will discuss some key parameters which are imperative to design a format-compliant encryption scheme. Finally, some related works will be evaluated.

A. Overview of H.264/AVC

In terms of classification, video encryption algorithms respect in a proportional manner certain criteria such as the efficiency of encryption, the security level, the conformity to standard video codecs and the compression efficiency. The latter two are closely related to the video compression process. In fact, the Standardized video compression technologies such as MPEG-1 (ISO/IEC, 1993) [5], MPEG-2 (ISO/IEC, 2000) [6], H.261 (ITU-T, 1993) [7], H.263 (ITU-T Recommendation H.263, 1998) [8], and MPEG-4 / H.264 AVC (Advanced Video Coding) (ITU-T Recommendation H.264, 2007, ISO/ IEC, 2005) [9] are widely deployed to economically store digital video on storage devices having limited ability or to effectively communicate on networks with limited bandwidth.

Most video coding standards use hybrid coding approach that consists on compressing the video data using simultaneously the "intra" and the "inter" encoding. Although there are differences among the applied coding algorithms, compression standards are built on the same set of basic operation elements.

H.264/AVC, known also as MPEG-4 Part10, has an enormous improvement in term of the compression performance. Thus, the compressed sequence is usually 30 to 50% shorter when compared to the previous MPEG-4 Part2 standard [4]. The block diagram of the H.264/AVC encoder/ decoder is presented in “Fig. 2”.

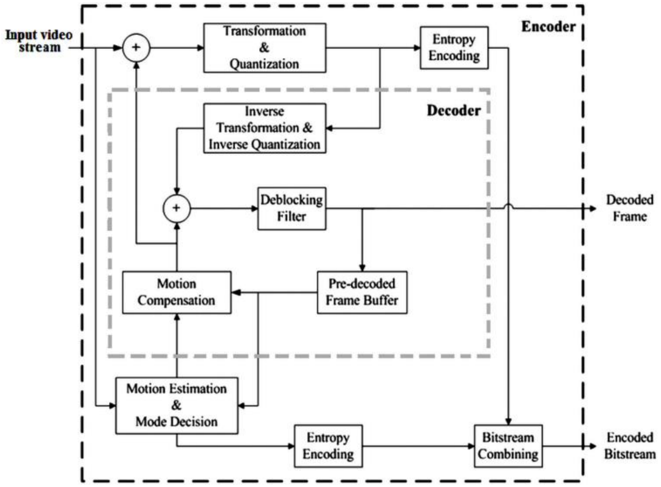


Fig. 2. Video Encryption Techniques

B. H.264/AVC Bitstream Syntax Structure

The main aim of the present research is to find a compromise between the speed of transfer and the preservation of a significant security level of multimedia data, while respecting the constraints that are imposed by the dedicated application (occupation, time, consumption ...). Accordingly, a mixed approach of encryption and compression is chosen in the present work. Thus, the cryptosystem must ensure not only confidentiality but also low power consumption and a very small occupation on FPGA. Furthermore, to ensure its integration into a compression sequence, different key parameters of the compression standard must be evaluated. This section is devoted to study the design constraints and various properties of the H.264 standard.

In fact, in a video stream, the data is presented in a hierarchical way. First, the video begins with a start code sequence (header). It contains one or more groups of pictures (GOP), and ends with an end code sequence.

The group of pictures (GOP) consists of a periodic sequence in the compressed images. In reality, there are three types of compressed images. The I-image (Intra) is compressed independently of the other pictures. The P-image (predictive) is coded using prediction of a previous image of type I or P. Finally, the B-images (Bidirectional) are encoded by double prediction using as reference a previous and next image of I or P type. A group of pictures starts with an I-frame, contains a periodic sequence of P-frames separated by a constant number of B-frames (see “Fig. 3”) [8][9].

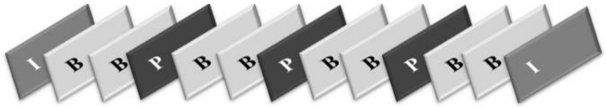


Fig. 3. The structure of a GOP

A GOP structure is defined by two parameters. These are the number of images and the distance between I-images and P-images. In fact, an I-image is inserted every 12 frames.

An image consists of three matrices where each matrix element represents a pixel. The YUV model defines a color space with three components. The first is the luminance and the others present the chrominance. The U and V matrices have smaller dimensions than the matrix Y (relatively to the used format). The most important information of the picture is stored in the matrix Y [8][9].

The image is cut in slices whose purpose is to limit the errors propagation in image transmission/storage. A slice is a sequence of macros blocs. A macro-block represents a portion of the image of 16 × 16 pixels size. A block is a 4 × 4 matrix of coefficients each one represents one of the three components of a pixel, Y, U or V [8][9].

“Fig. 4” below describes the hierarchical aspect of a video sequence from the GOP to the 4x4 blocks.

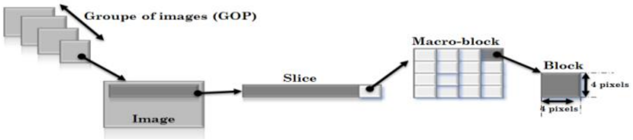


Fig. 4. Data hierarchy in a video stream

C. Key Parameters for a Selective Video Encyption

The process of video compression involves three processes: Discrete Cosine Transform (DCT), quantization and coding. To achieve the best choice of the location of the designed cryptosystem in the chain of compression, it is indispensable to take in consideration the execution time, the level of security, and the complexity of the system.

Observing the structure of a video encoder, we realize that if the proposed cryptosystem is placed after the DCT transformation, a decryption system is needed to be added in the decoder which aims to build on the temporal redundancies of a video streaming. The principle is to predict the content of an image and to encode only the error made in this prediction. Thus the existence of a cryptosystem increases the processing time and affects the complexity of the encoder. However, a cryptosystem inserted after the quantization step will not require an additional time for a decryption process.

In fact, the DCT is used to move the spatial domain to the frequency domain and also to collect as much information as possible in a small number of frequency coefficients. The DC coefficient shows the average of samples processed and presents the most important details in the raw of an image (lower spatial frequency). The AC coefficients represent the fine details of the image (higher spatial frequencies) [10].Thus, the DC coefficients carry more useful information than the high frequency components. Moving away from DC components of the image, not only the coefficients tend to have low values, but also, they become less important for the description of the image.

“Fig. 5” shows that the number of the DC coefficients represent (1 / 16) of all coefficients in a macro-block that contains 24 DC coefficients and 384 AC coefficients. Therefore, DC coefficients of an image I present (1 / 192) of the total coefficients. In consequence, if we assume that TG represents the required time to encrypt a video stream, hence the required time to encrypt only the I-frames of this flow will be reduced to (TG / 12) while maintaining a considerable security level. Moreover, if only the DC coefficients of I-frames are encrypted the required time for encryption process will be (TG / 192).

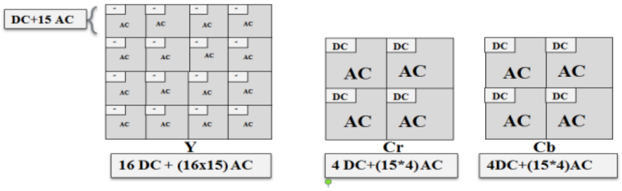


Fig. 5. The structure of 4 : 2 : 0 macro-blocks

Before defining the encryption scenarios, it is required to know the maximum number of different types of coefficients processed per second. It helps us to choose the most appropriate cryptographic algorithm. In this context, all the necessary calculations for the design of the proposed cryptosystem were performed. The following table I summarizes the obtained results.

TABLE I. KEY PARAMETERS FOR VIDEO ENCRYPTION

Group	max size of one image (mb)	DC coef Nbr in an image	AC coef Nbr in an image	max I images per seconde	max DC coef Nbr of I images (s)	max AC coef Nbr in I images (/s)	max DC coef Nbr (/s)	max coef Nbr (/s)
1	99	2376	35640	4	9504	142560	35640	570240
1b	99	2376	35640	4	9504	142560	35640	570240
1.1	396	9504	142560	2 or 9	19008 or 85536	285120 or 1283040	72000	1152000
1.2	396	9504	142560	6	57024	855360	144000	2304000
1.3	396	9504	142560	6	57024	855360	285120	4561920
2	396	9504	142560	6	57024	855360	285120	4561920
2.1	792	19008	285120	6	114048	1710720	475200	7603200
2.2	1620	38880	583200	5	194400	2916000	486000	7776000
3	1620	38880	583200	5	194400	2916000	972000	15552000
3.1	3600	86400	1296000	5	432000	6480000	2592000	41472000
3.2	5120	122880	1843200	4	491520	7372800	5184000	82944000
4	8192	196608	2949120	4	786432	11796480	5898240	94371840
4.1	8192	196608	2949120	4	786432	11796480	5898240	94371840

4.2	8704	208896	3133440	4	835584	12533760	12533760	200540160
5	22080	529920	7948800	5	2649600	39744000	14155776	226492416
5.1	36864	884736	13271040	5	4423680	66355200	23592960	377487360

D. Review of the Related Work

In this section, we will describe the currently known encryption algorithms for MPEG video streams in order to evaluate them with respect to three metrics: security level, encryption speed, and encrypted MPEG stream size.

In fact, several selective encryption schemes have been previously discussed in the recent past. In [11], an efficient encryption system for the H.264/Scalable Video Coding (SVC) codec is presented. The proposed selective encryption scheme is suitable for video distribution to users who have subscribed to differing video qualities on medium-to-high computationally capable digital devices. Another idea of a selective encryption on SCV is proposed in [12]. It involves the encryption of signs of coefficients, sign of motion vectors, and the alteration of DC values to ensure three different security levels. Although the sign encryption has no effect on the compression efficiency and the bitrate, the alteration of the DC values changed the video statistics and affected the compression efficiency.

In [13], the proposed scheme encrypts the video by scrambling the Intra-Prediction Mode (IPM) of intra macro-blocks. The main limit of this scheme is that it offers less security level due to the length of the pseudo number sequence. In [14], two fold video encryption techniques applicable to H.264/AVC are presented. In fact, the authors proposed an encryption of the DCT coefficients which affects the statistical characteristics of data. In addition, the compression ratio is affected which consequently increases the bitrate.

This paper proposes a combination of pseudo-random key generator and permutation code algorithm. The main objective is to enhance the security of H.264 video. In the next section, the proposed scheme is discussed in detail along with the generation of pseudo-random keys.

III. The Proposed Selective Encryption Scheme

The purpose of this work is the design of a cryptographic processor mainly dedicated to multimedia applications. The obtained cryptosystem will be placed on a prototyping platform based on FPGA to encrypt video transmissions in real-time conditions. In this context, the H.264 AVC part 10 standard is chosen. It is defined in most multimedia applications such as video conferencing, Internet video, media players, video mobile, and some satellite channels.

The design of the cryptosystem can be studied in two directions: The first one consists on proposing cryptographic protocols that should be appropriate for applications presenting time and security constraints. In the second direction, it is essential to realize the implementation of the system in a compression sequence that presents the constraints of the target application.

A. Design Flow

Designing systems with high architecture performance requires the choice of the most appropriate algorithms. Similarly, the definition of the design flow from functional level to physical level is a crucial step. It greatly affects the time of conception and the realization of the target system.

The proposed design flow is based on five strategic points. First, the definition of the requirements and the specification of the encryption techniques is an important step that consists on setting the goals of the project and studying the various constraints. The latter are related to target applications in order to ensure the conception coherence. Secondly, according to the study of the constraints imposed by the target applications, different cryptographic protocols will be proposed in order to achieve a hierarchy of security levels. Then, modeling the security IP requires architectural optimizations in order to adopt the cryptosystem to both application needs and used platform. Fourth, the logic synthesis and the performance evaluation of the designed cryptosystem ensure the validation of the proper functioning of the IP under real- time constraints. Finally, the hardware/software validation (Co-simulation) of the proposed cryptosystem verifies the architecture of the final prototype in a hardware environment. This will enable us to achieve real-time evaluation of system performance in terms of execution time and throughput. The tools provided by the reconfigurable platform and the electrical measurements allow us to evaluate the energy consumed by the proposed cryptosystem.

B. Proposed Cryptographic Scenarios

As mentioned before, encrypting the entire video is not always reasonable. This is mainly due to the large size of videos. Thus this kind of encryption approach is not recommended for embedded systems where the energy capabilities are limited. In such cases, saving time and energy consumption becomes an important issue. Hence, a selective encryption is compulsory. Accordingly, in this paper, four different encryption scenarios were proposed. They consist on encrypting only the most important data. In order to deal with the constraints of a real-time transmission, the least significant information will be switched while the most important data will be encrypted using a sufficiently secure algorithm. Therefore, the proposed scenarios are described below:

- The first scenario consists in encrypting the DC coefficients of the I-frames using an algorithm A. As shown previously, the images I carry the most useful information of the video stream. Hence, this scenario guarantees a high security level.

- The second scenario encrypts the I-frames. Thus, the DC coefficients of the I-frames are encrypted using an algorithm A while the AC coefficients are enciphered using an algorithm B. Therefore, this scenario has greater security level compared with the first scenario although it requires more execution time.

- The third scenario encrypts all the DC coefficients in the video stream using an algorithm A. Since the DC coefficients present the most important information of an image, this scenario provides a better security level.

- The fourth scenario consists in the encryption of the DC coefficients of all the images by an algorithm A and the AC coefficients of the I-frames by an algorithm B. This scenario provides a very high security level. However, it needs much execution time due to the large number of coefficients to be treated.

The table II summarizes the different proposed scenarios. It illustrates the speed, the security level, and the influence of encryption on the compression rate.

TABLE II. THE PROPOSED ENCRYPTION SCENARIOS

Scenarios	Treatments	Security level	Required execution time	Influence on the compression ratio
Scenario1	Only the DC coefficients of the I-images are encrypted.	**	*	*
Scenario2	The DC and AC coefficients of the I-images are encrypted	***	***	***
Scenario3	The DC coefficients of all the images are encrypted.	*****	**	**
Scenario4	The DC coefficients of all the images and the AC coefficients of the I-images are encrypted	******	****	****

Since the influence of the encryption on compression ratio depends only on the quantity of the encrypted data, the choice of encryption algorithms does not affect this parameter. However, while selecting the encryption algorithms, it is indispensable to take in consideration the coefficient nature and the desired security level which affect the encryption time and the compression ratio. Thus, in order to respect the constraints imposed by the characteristics of different levels and profiles, the choice of the encryption algorithms (A and B) must consider the speed of processing. Therefore, it is to guarantee a balance between the speed, the compression ratio, and the security level.

The table III shows the minimum speed needed to ensure the application of different scenarios. The minimum speed required for each treatment is equal to the maximum number of coefficients to encrypt multiplied by the size of a single coefficient (in bits).

TABLE III. THE MINIMUM REQUIRED SPEED FOR THE TREATMENT OF EACH SCENARIO

Scenarios	min speed required for the treatment (Mbit/s)
Scenario 1	53.084160
Scenario 2	849.346560
Scenario 3	283.115520
Scenario 4	1079.377920

C. Choice of the Encryption Algorithms

While encrypting a video stream, the transmission speed is a fundamental criterion. Therefore, the symmetric key algorithms are suggested to be used. In fact, the main disadvantage of asymmetric algorithms is that their treatment is slow. In addition, they require a lot of calculation. Therefore, their use becomes impossible for real-time applications. Concerning security, they present problems related to the structure of the public key systems. In fact, to ensure adequate security, the generated keys are larger in size compared to the symmetric key.

The main types of private key cryptosystems used today can be classified into two categories. These are the block ciphers that treat data blocks of fixed size and the stream ciphers that treat the data bit by bit. For the block cipher, good security is defined by a long key. This implies some drawbacks. In fact, the large blocks are safer but are heavier to implement. However, stream ciphers are very fast. The hardware implementation of the latter needs few gates, so they are suitable for real-time applications and often used to protect multimedia data. Generally, they are presented as a generator of pseudorandom numbers. A bit XOR is operated between the generator output and a bit from the data. However, the XOR is not the only operation possible.

In order to choose the appropriate key generator, a comparison between the most known stream ciphers has been made. We synthesized using the "Synplify Pro" component packages and the target component Virtex2 XC2v2000-6ff896. The table IV below summarizes the obtained results.

TABLE IV. COMPARISON BETWEEN PSEUDO-RANDOM GENERATORS

ciphers	Key size (bits)	Initialization Vector size(bits)	Frequency (MHz)	Occupation (Luts)	Consumption (mW)
A5/1	64	114	250.376	110	46.33
W7	128	128	188.590	777	111.77
CA 16×16	256	16	308.550	683	52.75
Grain-80	80	64	230.9	355	13.72
Grain-128	128	96	238.5	495	19.22

According to the table IV, we note the following observations:

- A5/1 has an acceptable speed and occupation rate (2%), and a relatively low consumption ratio. These results justify the use of this generator in GSM applications.
- The W7 frequency is the lowest. Whereas, its period is greater than that obtained by the other generators. Thus, it ensures a good security level.
- Grain consumption is the least compared to the other pseudo random generators. The frequency and the occupation values are acceptable for the real time

applications. However, its security level has to be checked.

Thus, randomness is very important to evaluate the quality of the generated keys. It presents one of the most critical points of configuring a crypto processor. In fact, to test quantitatively the randomness of the generated keys, the National Institute of Standards and Technology (NIST) announced, in 2001, a standard called FIPS 140-2. It covers four types of tests, namely, Monobit test, frequency test, Runs test and Longest test runs. A sequence is considered to be random if the probability P-value for each test is greater than 1% (0.01). The results of the various tests applied to the algorithms A5/1, W7, CA and Grain are presented in the following table V.

TABLE V. SECURITY TESTS OF PSEUDO-RANDOM GENERATORS

	Monobit test	**Frequency test**	**Runs test**	**Longest run test**
A5/1	0.0026 2^{64}	0.0028 2^{64}	0.0049 2^{64}	0.0021 2^{64}
W7	0.0022 2^{1024}	0.0016 2^{1024}	0.0046 2^{1024}	0.0025 2^{1024}
CA	0.0025 2^{256}	0.0018 2^{256}	0.0045 2^{256}	0.0010 2^{256}
Grain Standard Version	0.0109 2^{1024}	0.0101 2^{1024}	0.0131 2^{1024}	0.012 2^{1024}

The obtained results show that Grain provides a higher security level compared to the other well-known ciphers such as A5/1, W7, and CA. Grain provides higher security while maintaining a small hardware complexity. Accordingly, grain-80 will be used to ensure the key generation in the proposed cryptosystem.

As mentioned before, the cryptosystem will be integrated after the quantification step. Therefore, the AC and DC coefficients, resulting from the quantization step will be treated with appropriate systems and crypto-coded in order to achieve a crypto-compressed video. Thus, the DC coefficients will be encrypted using the key generated by Grain-80 while the AC coefficients will be switched. Fig. 6 illustrates the new Crypto-Compression Process.

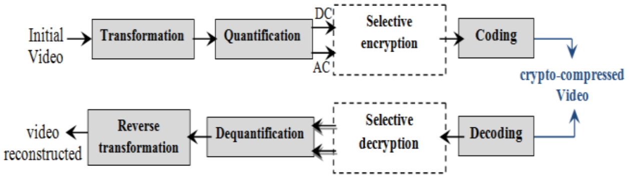


Fig. 6. Crypto-Compression Process

IV. DESIGN AND IMPLEMENTATION OF THE PROPOSED CRYPTOSYSTEM

From the system specification and cryptographic techniques, developed previously, it results the selection of the appropriate cryptographic algorithms as well as the location of the proposed cryptosystem in the compression process.

The implementation of the designed system is based on the complementarily of four different blocks. These are the Algorithm A (key generator: Grain-80), the configuration processor, the encryption processor, the re-configuration unit, and the permutation tables.

This structure allows for a good distribution of tasks between the blocks so that the proposed system can be adaptable to various applications. First, the key generation algorithm A and the permutation tables are defined with respect to the need. In addition, the function performed by the Encryption-module can be easily modified.

"Fig. 7" shows the general structure of the proposed system. In order to achieve the scenarios described above, Grain has been chosen as encryption algorithm to process the DC coefficients. The AC coefficients will be swapped using predefined permutation tables.

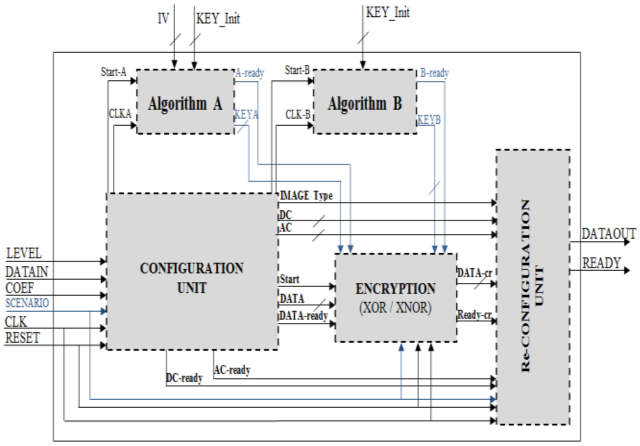


Fig. 7. The structure of the poposed cryptosystem

A. Grain Implementation

Grain is a stream cipher algorithm that appeared in 2005. It is designed to be very small and efficient in material implementation [15]. Gain family currently consists of two types of encryption. The first uses a key of 80 bits while the other uses a 128-bit key. Grain uses two registers. These are the LFSR (Linear Feedback Shift register) and the NFSR (Nonlinear Feedback Shift register). The output result is generated through a non-linear filter that takes two inputs of the shift registers. The following figure "Fig. 8" describes the structure of the Grain Stream Cipher.

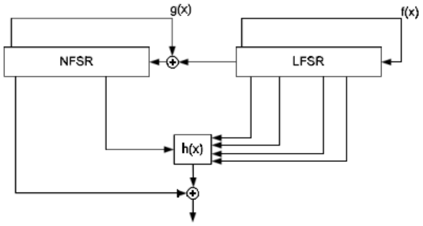


Fig. 8. The Grain cipher

The implementation and simulation of the Grain algorithm was achieved in VHDL. The Key Initialization phase ensures the initialization of the cipher using the initial key and the init-IV vector. This step is crucial before generating the key stream.

Grain is intended to be used in environments where gate counts and the power consumption as well as the memory needs to be very small. In fact, several ciphers are designed with better software efficiency compared to Grain. In fact, they are more appropriate when high speed in software is required.

In reality, the basic implementation has 1 bit/clock rate. The speed of a word oriented cipher is typically higher since the rate is 1 word/clock. Grain is a bit oriented cipher but it has compensated this problem by the possibility to increase the speed. Accordingly, a designer could choose the appropriate speed of the cipher according to the amount of hardware available. The following “Fig. 9” illustrates the cipher process when the speed is doubled.

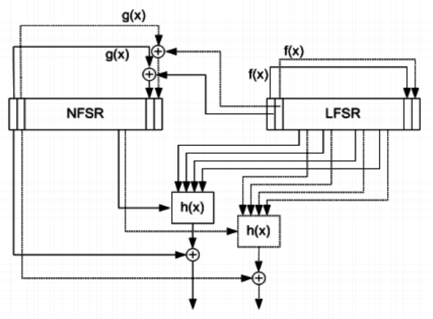


Fig. 9. The cipher process when the speed is doubled

We implemented all the possible versions of Grain-80 in order to choose the appropriate speed and performances for the target application. The synthesis results presented in table VI proved that the speed changes proportionally to the occupancy. In addition, the consumption ratio becomes increasingly significant from one version to another. For example from the standard version of Grain to Grain-16 version (where the speed is multiplied by 16), the change in consumption is negligible compared to the evolution of the speed (≈7x230.9 = 1652.8 Mb/s). The generic version gives the opportunity to choose the version that is compatible with dedicated applications, but it has a loss in speed, frequency and occupation. For example, compared to the original version the frequency of the generic version (with N=1) decreases from 230.9 to 39.9 MHz, while the occupancy reaches a value equal to 4533 Luts (≈12x 336).

TABLE VI. SYNTHESIS RESULTS OF GRAIN STREAM CIPHER 80

Grain Version	Frequency (MHz)	Occupation (Luts)	Consumption (mW)	Throughput (Mbps)
1	230.9	336 (<1%)	13,72	205,1
2	167,2	369	13,01	334,4
4	154,7	424	13,87	618,8
8	144,8	562	14,81	1158,4
10	148,3	664	14,84	1483
16	101,1	1035	18,58	1617,6
N	39,9	4533(9%)	15,95	(39,9*n)

According to these results, it is clear that each version has its own characteristics. Thus, choosing the appropriate version is based on the constraints of the target application. The proposed cryptosystem is dedicated to the real-time video application. Thus, the version Grain-V4 was chosen where the speed is multiplied by four.

B. *Configuration and Re-Configuration Units*

The scenarios configuration and assignment are carried out by the configuration module. It ensures three important functions. These are the level identification, the scenario specification, and the classification of images and coefficients. “Fig.10” illustrates the process of this unit.

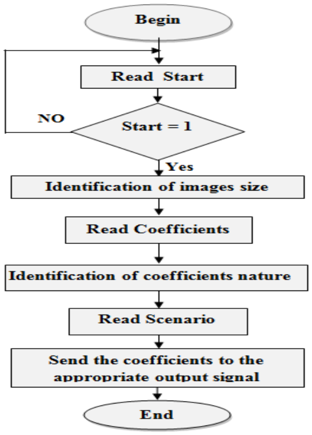

Begin
Read Start
NO
Start = 1
Yes
Identification of images size
Read Coefficients
Identification of coefficients nature
Read Scenario
Send the coefficients to the appropriate output signal
End

Fig. 10. The configuration unit process

The configuration module is fundamental in order to ensure synchronization between the other modules. Similarly, the reconfiguration module's role is to restore the flow of input coefficients and to reconstitute the encrypted video streaming.

C. *Encryption Unit*

This block is responsible for performing an XOR or an XNOR operation between the key generated by Grain-V4 and the coefficients to be encrypted (in case of DC coefficients). The AC coefficients are swapped using predefined permutation tables.

The encryption key generated by Grain is 80-bit size. Therefore, it can serve to encrypt 6 different DC coefficients. To improve the robustness of the proposed cryptosystem, two different functions were chosen to be performed. These are the XOR and the XNOR.

Since Grain takes 20 clock cycles to manage its first key, it is needed to manage the first coefficients reaching this block before the generation of the cipher key. However, after 20 clock cycles only 2 DC coefficients and 18 AC coefficients are ready for encryption. Thus, two registers have been defined to ensure this task.

D. *Permutation Unit*

As previously mentioned AC coefficients are switched following permutation tables that were defined for this purpose. Only 16 permutation tables were chosen to meet the design requirements. First, it is important to reduce the used memory in order to consume less in terms of occupation. Secondly, the key generated by GRAIN can be used to define only 6 different addresses (if the number of tables increases, more than 4 bits will be needed to represent the table number). In fact, 50 different tables were generated (based on Grain keys). Then, four different cryptographic tests were applied in order to evaluate the cryptographic properties of the generated tables. These are the nonlinearity, the strict avalanche criterion (SAC), bijection, and the BIC (output bits independence criterion). In fact, the generated tables satisfy the requirement of bijectivity since they have different output values. In addition, the average value of nonlinearity of the 16 generated tables is equal to 102. Furthermore, the mean value of the dependence matrix (SAC) of the chosen tables is equal to 0.5281 which is very close to the expected value 0.5. All these results justify the choice of the used permutation tables.

The following “Fig. 11” illustrates how the Grain key is used to choose the permutation table for the encryption process. In fact, the same table cannot be used to encrypt two successive blocks of data.

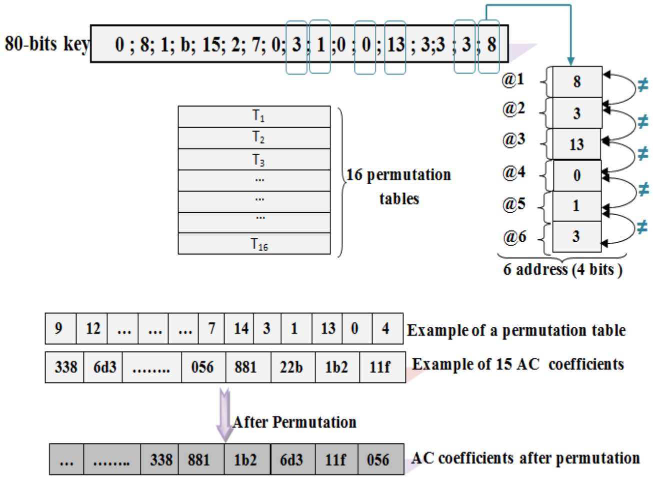

80-bits key
0 ; 8; 1; b; 15; 2; 7; 0; 3 ; 1 ;0 ; 0 ; 13 ; 3;3 ; 3 ; 8
T₁
T₂
T₃
...
...
...
T₁₆
16 permutation tables
@1
@2
@3
@4
@5
@6
8
3
13
0
1
3
≠
≠
≠
≠
≠
6 address (4 bits)
9 12 … … … 7 14 3 1 13 0 4
Example of a permutation table
338 6d3 …….. 056 881 22b 1b2 11f
Example of 15 AC coefficients
After Permutation
… …….. 338 881 1b2 6d3 11f 056
AC coefficients after permutation

Fig. 11. The choice of the permutation tables

E. Synthesis of the Proposed Cryptosystem

Synchronization between system units is an imperative operation. In fact, the management of the clock has a fundamental role in system performance such as its total consumption. In this context, the Grain cipher is activated all throughout the treatment, although it is used only for specific times to encrypt DC coefficients. This gave us the idea to design a second version in order to optimize the used resources.

The Grain process was examined in order to be activated only when a key is needed. The management of the activation and deactivation of this generator allows us to use all the produced keys and to benefit of the provided security level. In the same context, the "Encryption" block can be activated in need. To manage the activation and deactivation of these two blocks, we used a clock generation processor which was implemented in the configuration block.

Moreover, different improvements have been carried out in order to optimize the used resources in the proposed cryptosystem. To evaluate the impact of these modifications, the synthesis of the proposed cryptosystem was performed using the component packages "Synplify Pro 9.6" and the target component Virtex5-XC5VLX50-FF676. The obtained results are presented in table VII.

TABLE VII. SYNTHESIS RESULTS OF THE DIFFERENT UNITS OF THE PROPOSED CRYPTOSYSTEM

	Configuration Unit	Grain V4	Encryption unit	Reconfiguration Unit
Occupation (Luts)	256 (1%)	282 (<1%)	157 (<1%)	28 (<1%)
Frequency (Mhz)	155.1	623.6	348.8	532.3

It is clear that the occupation of the different blocks is very small. This is due the division of labors and the use of procedures. For example, the synthesis of block "Encryption" gave the value 18 262 LUTs (95%) as occupation. However, after using the proposed modifications, the occupation has become equal to 157 LUTs (<1%). Furthermore, the frequency increases from 102.8 MHz to 160.3 MHz due to the proposed improvements. The following table VIII summarizes the obtained results.

TABLE VIII. SYNTHESIS RESULTS OF THE PROPOSED CRYPTOSYSTEM

	Optimized Cryptosystem	Original Cryptosystem
Occupation (Luts)	722(2%)	18 827(97%)
Frequency (Mhz)	160.3	102.8

To conclude, we can claim that the optimized cryptosystem has good performance in terms of occupation, frequency and consumption. It increases with the amount of information processed and the complexity of the applied scenarios. The results justify the implementation the optimized version in the validation phase.

V. THE HARDWARE/SOFTWARE VALIDATION

The objective of this section is to check that the hardware and software specifications are valid. This involves testing and studying the evolution of the cryptosystem in the presence of environmental constraints such as the throughput, the implementation costs, and the execution time. The verification includes the examination of the running of the designed system. In fact, it can be simulated and tested at the behavioral level through an ordinary simulation tool such as "ModelSim". Then, the obtained synthesizable IP (Intellectual Property) can be frozen in hardware (FPGA or ASIC). Accordingly, the implementation of the proposed cryptosystem on the reconfigurable platform will allow for an assessment of the occupied area as well as the real-time constraints.

Since, the integration of an IP Core in a real-time hardware design is a complex task; an efficient methodology for the real-time implementation on a reconfigurable platform is required. In fact, the flow consists in developing and synthesizing the appropriate IP to be integrated through the Xilinx System Generator tool in the EDK flow which is used to transform the RTL implementation into a complete FPGA implementation [16-18]. Once the IP is valid, it is integrated and exported as a PCORE to the Platform Studio Project. Finally, the communication between the Micro Blaze processor and the PCORE has to be made. It provides a Hardware/Software Co-Simulation environment to test the embedded system design. This communication often occurs over shared bus connectivity.

The following “Fig.12” illustrates the conception flow of a real-time design for the proposed cryptosystem.

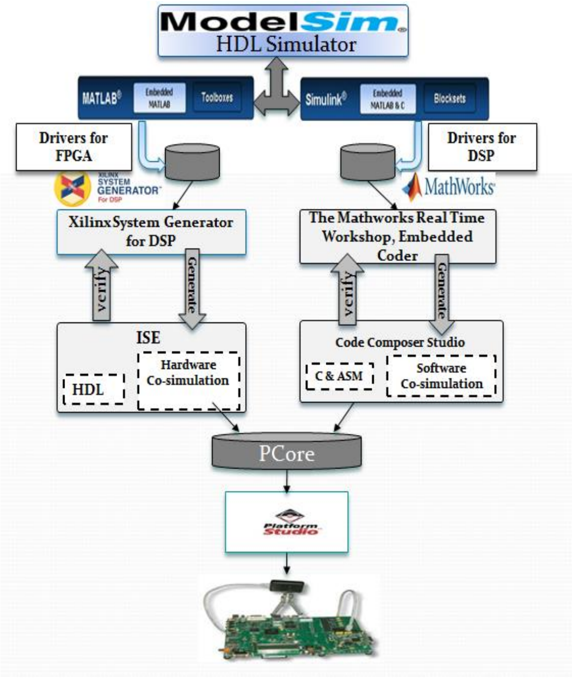


Fig. 12. The choice of the permutation tables

The System Generator provides a hardware co-simulation to incorporate an architecture running on the FPGA directly in a Simulink simulation. The video model tested and verified in the previous step, must be compiled for hardware co-simulation. The selection of the target platform for the compilation must be made. In fact, Spartan 3A DSP 3400 Platform offers us the opportunity to implement and verify the hardware implementation results.

A. *Integration of the Proposed Cryptosystem in the H.264 Encoder*

Zexia provided H.264 encoder implemented in VHDL [20]. It is designed as a modular system with small and efficient components using low power ressources. The proposed cryptosystem was integrated in the Zexia-H.264-encoder in order to validate its process. The following figure 13 shows the structure of the obtained crypto-encoder.

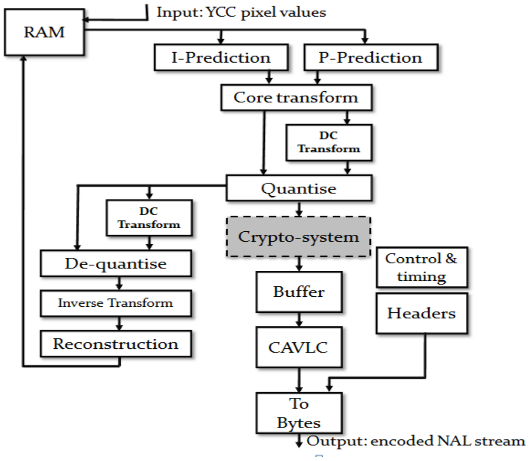


Fig. 13. Architecture of the new crypto-compression system

The proposed cryptosystem is adapted in order to be integrated into the compression process. “Fig.14” shows the simulation results of the obtained crypto-compression system. It presents the major signals of the different blocks when the fourth scenario is applied to encrypt the video stream.

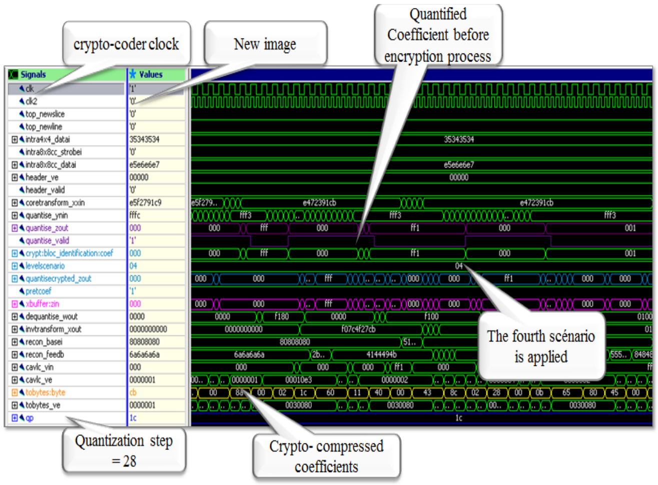


Fig. 14. Simulation results of the optimized crypto-compression system

B. *Integration of cryptosystem model of Camera Design*

This section presents the integration of the proposed cryptosystem, developed in VHDL, using the System Generator Black Box in the model of camera design. In fact, the reference design was used. It includes a VSK-Camera-VOP Bayer filter to restore the image in RGB format. The generated PCORE is exported as a new EDK-PCORE in the proposed project. The design shown in “Fig.15” consists of the Starter Kit video (VSK) Spartan 3A DSP FPGA XCSD3400A. This card is used to decode the data that came through the serial port interface LVDS Camera.

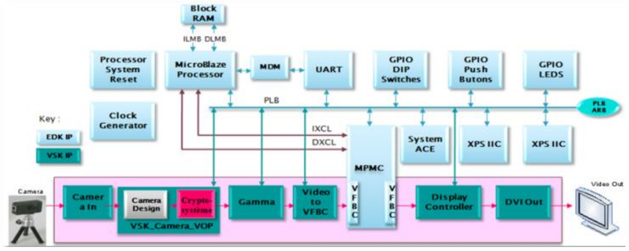


Fig. 15. Architecture of the integration of hardware cryptosystem in the Design of Camera Frame Buffer

"Fig.16" shows the external structure model VSK-Camera-VOP and "Fig.17" details its internal structure.

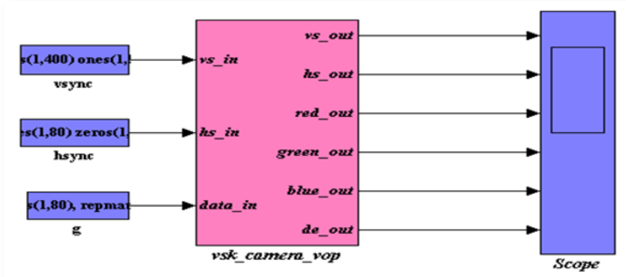


Fig. 16. external structure of VSK-Camera-VOP model

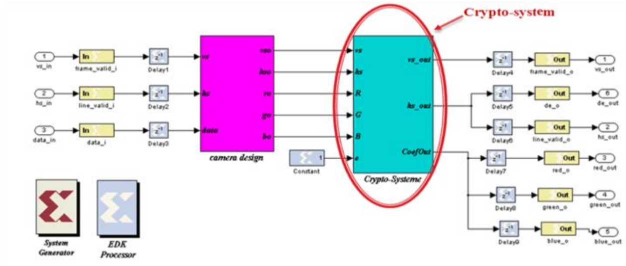
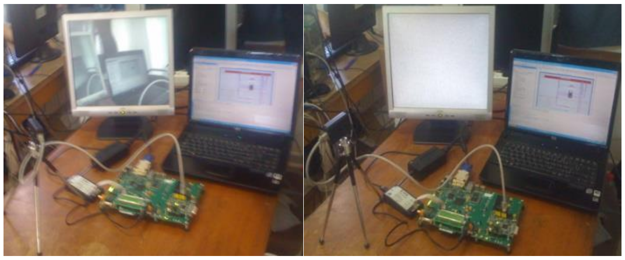


Fig. 17. internal structure of VSK-Camera-VOP model

C. *Real time validation on Spartan 3A DSP platform*

In the Hardware Co-simulation of real-time cryptosystem, the string contains the entire cycle of acquisition, processing and retrieval of a video signal from a video source (camera). The results of the Hardware Co-simulation presented in the following "Fig.18", allow us to verify the efficiency and the robustness of the proposed model HDL.



(a) original video (b)encrypted video

Fig. 18. Real time validation on Spartan 3A DSP platform

Image processing in real time requires the use of fast electronic circuits that are capable of handling large amounts of information generated by the video source. That's why FPGAs are ideal for this kind of application.

D. *Security analysis*

In order to analyze the security of the proposed cryptosystem against most known attacks, security tests were conducted on Foreman video (352x288, 164 frames). Then, the entropy values, the PSNR (Peak Signal-to-noise ratio), and the Horizontal and vertical correlation coefficients were observed.

- The correlation provides a quantitative representation of the similarities between the original and the encrypted frames. In fact, low correlation coefficient indicates that there is less similarity between the original and encrypted video, which shows the efficiency of the encryption scheme.
- The PSNR is the most widely used metric to estimate image distortion measure. This metric compares the visual quality between the plain image and the ciphered one. The PSNR is based on the Mean Squared Error value (MSE) that delivers the error between two images.
- The information entropy is one of the most important features of randomness. In fact, the source is considered to be truly random if the information entropy of the ciphered image is close to eight.

The following table IX presents the different analysis results. They justify the efficiency of the proposed cryptosystem.

TABLE IX. SECURITY ANALYSIS OF THE DIFFERENT PROPOSED SCENARIOS

	Horizontal correlation	**Vertical correlation**	**PSNR value (dB)**	**Information Entropie**
Scenario 1	0.0883	0.2201	16.42	7.4928
Scenario 2	0.0844	0.0974	14.8842	7.5580
Scenario 3	0.0732	0.0824	12.5028	7.5595
Scenario 4	0.0585	0.0778	9.9642	7.6956

VI. CONCLUSION

In this paper, a new cryptosystem dedicated for multimedia applications is proposed. It is designed to be integrated into the H.264 encoder. It provides four different encryption scenarios. The proposed structure is essentially based on a pseudo-random generator, a configuration unit and an operator performing an XOR/XNOR between the generated keys and the appropriate data which are identified by the configuration processor. This operator is also responsible, of the data swapping based on highly nonlinear permutation tables.

The choice of cryptographic algorithms was based on the study of environmental constraints imposed by the targeted applications such as the real-time transmission, the speed, the influence on the compression ratio and the desired security level. Hence, Grain-80-V4 was chosen to encrypt the DC coefficients which have the most important information of the video stream. The permutation was elected to encrypt the AC coefficients that are more numerous than the DC coefficients.

In order to deal with the real-time multimedia applications, we chose the joint compression and encryption approach that does not require too much time for encryption/decryption process while maintaining a considerable amount of compression ratio.

Several perspectives emerge as a result of the present research. In fact, it is important to study the resistance of the proposed cryptosystem against certain types of attacks such as the fault injection attacks. Appropriate counter-measures should be proposed if necessary. In addition, the chaos-based selective encryption is a new and an efficient approach used for the multimedia application. It is attracting an increasing research effort due to its favorable properties such as the good pseudo randomness and the high sensitivity to the initial values.

References

[1] B. Furht, D.Kirovski, ‘’Multimedia Security Handbook’’, CRC Press LLC in December 2004.

[2] S. Lian, Multimedia Content Encryption: Techniques and Applications (Taylor & Francis Group, LLC, 2009).

[3] Z. Shahid, M. Chaumont, and W. Puech, “Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames,” IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 5, pp.565-576, May 2011.

[4] Li, Y., Liang, L., Su, Z., Jiang, J., “A new video encryption algorithm for H.264”, Fifth International Conference on Information, Communications and Signal Processing (ICICS), pp. 1121–1124, IEEE 2005.

[5] ISO/IEC 11172-2. Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s: Video, 1993.

[6] ISO/IEC 13818-2. Information technology–generic coding of moving pictures and associated audio information: video, 2000.

[7] ITU-T Recommendation H.261. Video code for audiovisual services at px64 Kbit/s, March 1993.

[8] ITU-T Recommendation H.263. Video coding for low bit rate communication, Feb. 1998.

[9] ISO/IEC 14496-10. Information technology–coding of audio–visual objects–Part 10: advanced video coding, 2005.

[10] Richardson, E.G., “H.264 and MPEG-4 Video Compression–video coding for nextgeneration multimedia”, 1st ed. John Wiley & Sons, New York, 2003.

[11] M. Asghar, M. Ghanbari, M. Fleury, and M. Reed, “Efficient Selective Encryption with H.264/SVC CABAC Bin-Strings”, 19th IEEE International Conference on Image Processing, IEEE,2011.

[12] G.B. Algin, and E.T. Tunali, “Scalable video encryption of H.264/AVC codec,” J. of Visual Commun. and Image Representation, vol. 22, no. 4, pp. 353-364, 2011.

[13] Siu-Kei Au Yeung et al, “Partial Video Encryption Based on Alternating Transforms”, IEEE Signal Processing Letters, vol. 16, No. 10, pp. 893–896, October 2009.

[14] T.Chattopadhyay and Arpan Pal, “Two fold video encryption technique applicable to H.264 AVC”, IEEE International Advance Computing Conference, pp. 785 – 789, March 2009.

[15] S.S. Mansouri, E. Dubrova, “An Improved Hardware Implementation of the Grain Stream Cipher”, 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools (DSD), pp. 433–440, IEEE 2010.

[16] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, San Vo, “A statistical test suite for random and pseudo-random number generator for cryptographic applications”, NIST Special Publication 800-22.

[17] Xilinx, “Embedded System Tools Reference Manual”, EDK 10.1, Service Pack 3, 19 September 2008, www.xilinx.com/support/documentation/sw_manuals/edk10_est_rm.pdf.

[18] Xilinx, “System Generator for DSP Getting Started Guide”, UG639 (v11.4), December 2, 2009, www.xilinx.com/support/documentation/sw_manuals/xilinx11/sysgen_gs.pdf

[19] Xilinx, “Spartan-3A DSP FPGA, Video Starter Kit” UG456 (v2.1) March 15, 2010, www.xilinx.com/support/documentation/boards_and_kits/ug456.pdf.

[20] Zexia Access Ltd © 2008 - H.264 Hardware Encoder: http://hardh264.cvs.sourceforge.net/viewvc/hardh264/hardh264/src