Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Overview of securing multimedia content using efficient encryption methods and modes

K. John Singh *, Kunal Gagneja

School of Information Technology and Engineering, VIT University, Vellore, India

ARTICLE INFO

Article history:
Received 27 May 2017
Received in revised form
17 August 2017
Accepted 25 August 2017

Keywords:
Partial encryption
Scalable encryption
Perceptual encryption
Compression combined encryption
Video scrambling
Hardware

ABSTRACT

Multimedia comprises of audio, text, image and video. Use of multimedia is increasing because of improvements in hardware, algorithms and networking. Confidentiality of data is the primary concern due to applications in commerce, telemedicine, Internet television, video telephony, multiparty P2P conferences, video on demand and military. Multimedia files are data intensive thus, they need more computational power and consume more memory as compared to ordinary text data. Comparative analysis of vulnerabilities and counter measures are made. In this paper, possibilities of securing multimedia data using various encryption methods and modes are analyzed and compared on the basis of their execution speed, hardware implementation and various attacks. It is found that public key cryptosystems are comparatively slow and they get more vulnerability. Comparative analysis shows that confusion and diffusion are used in many faster cryptosystems to measure the security level. Moreover, hardware implementation (ASIC and FPGA) provides better security than software implementations. ASIC and FPGA implementations had high variation in throughput irrespective of the cryptosystem.

1. Introduction

Multimedia is the presentation of data in more than one form. Some of the examples are audio, text, animation, images, interactive content and video. Animation includes aspect of time too. Video is time oriented creative media. Once Apple CEO said that multimedia is not a market. It is a technology. Today there is no multimedia market, because everything is multimedia. One if its advantages are capability to transfer more amount of information to audience in same time.

Naive algorithm approach is a straightforward approach, which encrypts compressed content with a conventional cryptographic method such as AES (NIST, 2001). Conventional algorithms generally aim at text encryption and are not suitable for video encryption because they cannot process large amount of data securely in less time. It is not possible to adapt them to paradigms, which require special adjustments for example perceptual encryption (Joshi and Dalal, 2012) in Video on Demand. Specific encryption algorithms permit simultaneous encryption and decryption, reducing processing burden and allow more users in network. Challenges in multimedia encryption are high redundancy, oblivious detection, time efficiency and real time operations in context of video calls.

Reduction in data volumes using compression and faster encryption algorithms are the methods for attaining higher time efficiency. Cryptographic security refers to security against cryptographic attacks for example ciphertext-only attack, known-plaintext attack and brute force attack. Multimedia has improved the quality of education and journalism too. However, widespread use and importance in sensitive conditions such as diplomatic and international conferences between governments has raised questions about integrity and confidentiality. Examples of network multimedia include PSTN, World Wide Web, medical imaging, electronic publishing, exchange of music or video files, work at home and radio. It is important for formats for be compatible with sender and receiver in such applications.

1.1. Importance of multimedia security

Multimedia security is required because of increasing use of cloud, distributed systems, satellite video, robotic surgery, drones and video calls. The

* Corresponding Author.
Email Address: johnsinghaj@yahoo.com (K. J. Singh)

https://doi.org/10.21833/ijaas.2017.010.013
2313-626X/© 2017 The Authors. Published by IASE.

nature of multimedia data makes it vulnerable to side channel attacks. Comparatively larger keys are required because of the nature of multimedia data. Because of decreasing hardware costs, it has become easy to infringe copyrights of commercial and noncommercial multimedia content. Conditional access systems, which are used for terrestrial, cable and satellite distribution, also need to be protected from eavesdropping. For example, some virtual reality systems are geographically separated. Secure communication is essential to ensure reliability and protection in distributed multimedia networks. Nowadays, multimedia networks are distributed, yet data centric. Moreover, they are redundant, collaborative, autonomous, application-specific, resource constrained and hierarchical. Various types of attacks are possible in multimedia data transmission. For example, snooping attack in which an eavesdropper monitors the link between content owner and replicated end. This attack becomes more severe if content is unencrypted. Authentication, watermarking, digital signature, access control and stenography are some of the methods of attaining security.

2. Encryption methods and modes

Encryption algorithms can be classified as symmetric and asymmetric encryption algorithms. Symmetric key algorithms are also called single key, one key, private key and conventional encryption algorithms. Symmetric key ciphers have higher throughput, which can go up to gigabytes per second in hardware implementations. As compared to public key encryption, same level of security can be achieved with shorter keys; however key generation and handling are still an issue of active research. Comparatively longer keys are required for digital signatures. Encryption and decryption keys are same in symmetric key ciphers. In asymmetric ciphers, public key is used for encryption, and however, only private key can decrypt the cipher text. Public key is known to everyone, but private key is known only to receiver.

This is the reason why public key encryption algorithms have more vulnerability. Generally, symmetric ciphers are more secure, with disadvantage of key distribution. They are faster in software implementations, making them more popular in encryption of large files. Public key cryptography is slower, has longer keys and is more suited for secret key exchange. RSA, Diffie-Hellman, Elliptic Curve Cryptography and Elgamel are asymmetric key cryptosystems. Thus, symmetric and asymmetric cryptosystems complement each other. Architectures of symmetric and asymmetric ciphers are as shown in Figs. 1 and 2 respectively.

Algorithms can also be classified based on block ciphers and stream ciphers. Block cipher can be used to create message authentication code, keyless hash function and stream cipher (Hudde, 2009; De Canniere, 2006). Stream cipher can be generated from block cipher by padding. Block ciphers encrypt blocks of data, which can be 64, 128 or 256 bits long (Knudsen and Robshaw, 2011).

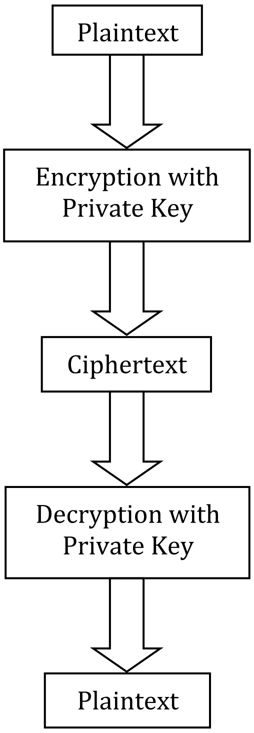

Fig. 1: Symmetric key encryption

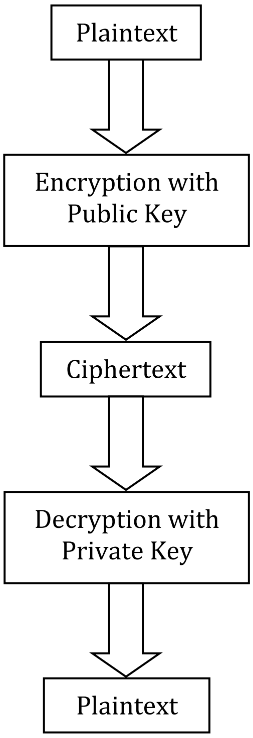

Fig. 2: Asymmetric key encryption

Stream ciphers encrypts in streams of bits. It is assumed that generally stream ciphers, which are used in applications requiring higher throughput, are twice as fast as block ciphers (Bondanov, 2007). However, latest block ciphers have proved to be more efficient. In past few years, block ciphers have become more popular as compared to stream ciphers because of more security. For example, A5/1, which is used in GSM standard, is a stream cipher.

However, A5/3, which is its successor, is a block cipher (De Canniere, 2006). IEEE 802.11 or wired enhanced privacy is uses RC4, a stream cipher. IEEE 802.11i uses AES, a block cipher for encryption. Table 1 shows classification of multimedia encryption algorithms based on architecture.

Encryption modes are designed to ensure confidentiality and integrity. Cipher block chaining, cipher feedback mode, counter mode, electronic codebook mode and output feedback mode are the encryption modes used in multimedia encryption. ECB, CBC, CFB and output feedback mode are used by block ciphers such as 3DES, DES, Twofish, AES, RC2, Rijndael, IDEA, RC5, Skipjack algorithms, secure socket layer and VPN (Young and Aitel, 2003). However, counter mode is used with DES and AES (Paar and Pelzl, 2009). They are explained in Table 1.

Table 1: Classification of encryption techniques

Algorithm	Block/Stream Cipher	Symmetric /Asymmetric key
AES	Block	Symmetric
DES	Block	Symmetric
A5/1	Stream	Symmetric
Blowfish	Block	Symmetric
Cast 256	Block	Symmetric
Twofish	Block	Symmetric
Ice	Block	Symmetric
Mars	Block	Symmetric
Misty1	Block	Symmetric
RC2	Block	Symmetric
Tea	Block	Symmetric
Serpent	Block	Symmetric
Triple Des	Block	Symmetric
RC4	Stream	Symmetric
RC6	Block	Symmetric
RSA	Block	Asymmetric
Seed	Block	Symmetric

2.1. Cipher block chaining

CBC is progressive encryption algorithm. CBC MAC combines CBC with message authentication code (Bellare et al., 1994). Chaining is used to add feedback mechanism to block ciphers. Encryption results of previous blocks are required to encrypt the current block. Each cipher text block is XORed with next plaintext before encryption. Feedback register is used to store ciphertext. Plaintext block is XORed with feedback register to derive input for encryption routine. It continues until the entire plaintext is encrypted. However, it can result in error propagation, because an error in bit stream may result in incorrect encryption and decryption for consecutive blocks. It is used for encryption of videos and images containing high redundancy (Furht and Kirovski, 2004). At time of decryption, earlier block is decrypted irrespective of later block is available or not. Architecture of CBC mode is shown in Fig. 3.

2.2. Cipher feedback mode

It provides automatic resynchronization by modifying block cipher as a stream cipher, which is self-synchronizing (Heys and Zhang, 2011). Ciphertext bits are fed back to derive the input. It is not used with AES in hardware and software because of its low speed. CFB is used when block length is less than minimum block length. Padding is not required because a block may be as long as a bit or few bytes. 64 bit shift register is filled by a random number i.e. initialization vector. First "x" bits are selected from plaintext block and are XORed with plaintext. Output is sent as input to shift register. Detailed architecture is as shown in Fig. 4.

2.3. Counter mode

Parallel encryption can do without padding in counter mode. CTR is used in IPSec and Asynchronous Transfer Mode. A non-repeating counter, which is equal to plaintext block, is used. Counter value is incremented by one for each subsequent block. Encrypted counter is XORed with plaintext block without chaining to produce ciphertext. Encrypting different plaintexts with same input must be avoided because an eavesdropper can calculate key stream block, which can be used for further decryption. Assuming 128 bit AES has 96 bit nonce. Counter Encryption process is as shown in Fig. 5.

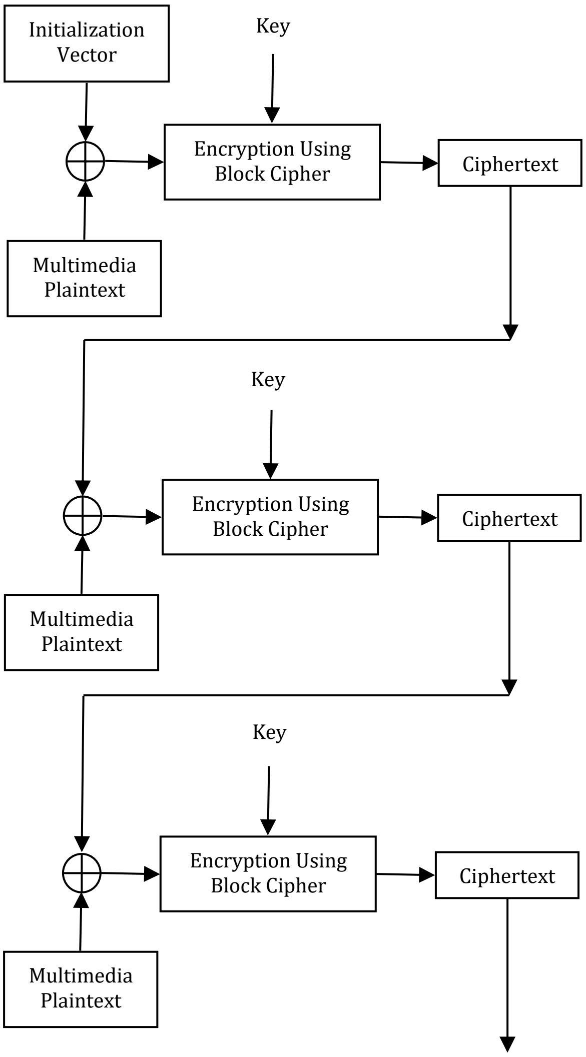

Fig. 3: Architecture of CBC mode (Gregory, 2015; Gunasekera, 2012)

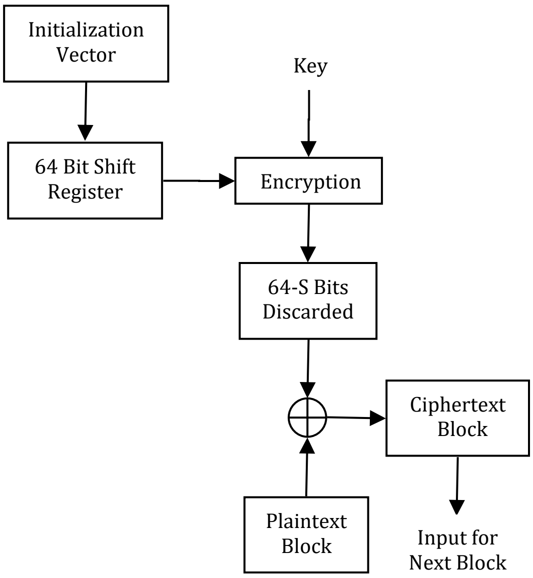

Fig. 4: Cipher feedback mode (Stallings, 2006)

2.4. Electronic codebook mode

Blocks are encrypted or decrypted independently, thus errors in one or more bits are restricted to that block only (Delfs et al., 2002). It is insecure, partial and deterministic method of encryption. Identical plaintext blocks result in identical ciphertext blocks, making it even more insecure in context of high definition video files, where redundancy is high. Increase in ciphertext makes it more insecure and that is why, it is generally avoided. Fig. 6 shows output after encryption with ECB mode. Ciphertext image has many similarities with plaintext image.

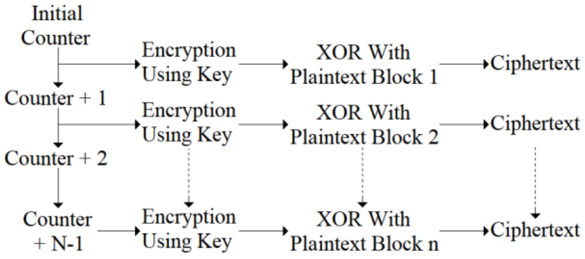

Fig. 5: Counter mode of encryption (Pachghare, 2015)

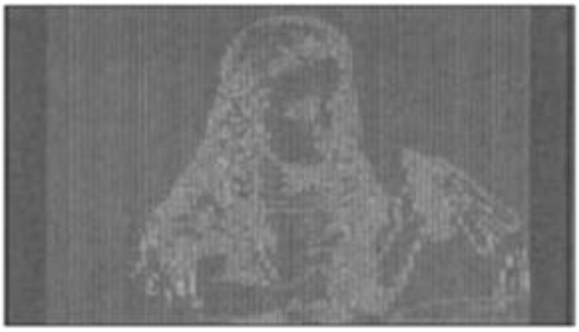

Fig. 6: Insecure ciphertext image after electronic codebook mode (Stamp and Low, 2007)

2.5. Output feedback mode

This mode has less error propagation since one bit error in ciphertext causes error of only one bit in plaintext. Initialization vector is required by OFB for initializing n-bit input block. Encryption and decryption methods are same. Output of this mode is independent of cipher text and plaintext. A new IV is required between sender and receiver to obtain synchronization, in case it is lost. OFB process for DES encryption for video scrambling and descrambling is shown in Fig. 7.

3. Types of encryption techniques

Plaintexts are often of large volume, real time operations, compressed data and high redundancy (Sasaki, 2007). Efficiency is required so that access operations and transmissions are not delayed. Use of lightweight encryption algorithms and reduction in encrypted data volumes are the methods used for attaining efficiency. Compression ratio must be kept constant to reduce transmission bandwidth or storage space. Direct encryption, partial encryption (Zeng and Lei, 2003) and compression-combined encryption are the encryption methods for multimedia encryption. In direct encryption, novel or traditional cipher is used to encrypt compressed or uncompressed multimedia content directly (Mao et al., 2004).

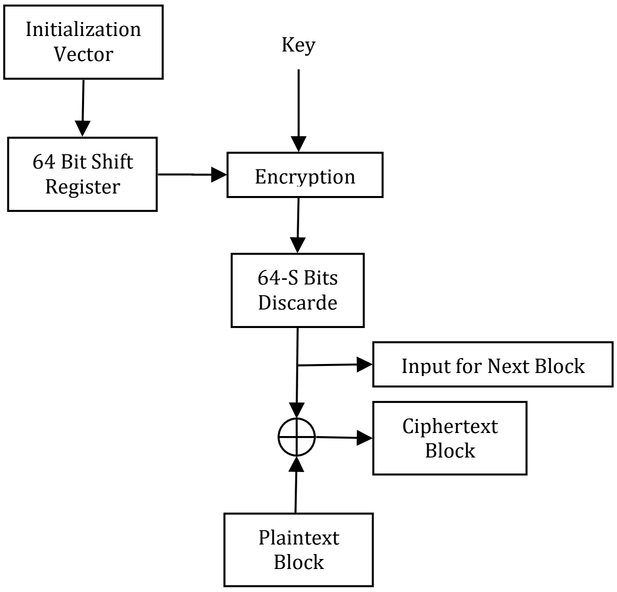

Fig. 7: Output feedback mode (Pachghare, 2015)

Scalable encryption which is used in media transcoding progressively encrypts in layers (Zhu et al., 2005). Format compliant encryption, which encrypts without format information depends on kind of use of algorithm. Format information is used to resynchronize transmission in environments with high error rates. Decoder uses file header, frame header, file tail, and so forth to realize synchronization. Format compliant encryption, format independent encryption, direct-operation supported encryption and communication compliant encryption are the types of algorithms, which are used for wireless encryption. First one combines encryption with compression, whereas, media data of arbitrary format is supported in second one. Third one supports direct operations on encrypted multimedia data, while transmission errors are considered in the fourth one. Format independent encryption algorithms assume multimedia data to be binary data and encrypt irrespective of file format. DES, IDEA, AES and RSA are some of the examples. They are included in protocols such as secure socket layer, IP security and package CryptoAPI.

Naive algorithm approach is the most common method, which encrypts video after compression. Perceptual encryption algorithms are more suited for video on demand (Li et al., 2007). Video encryption algorithms can be classified as joint compression and encryption algorithms and compression independent algorithms depending on whether compression is used or not (Liu and Koenig, 2010). Some of the requirements of video encryption are security (Wen et al., 2002), encryption efficiency (Liu and Koenig, 2005), direct operations, syntax compliance (Macq and Quisquater, 1995), perceptual encryption, video codec compliance and compression efficiency. Syntax compliance, which is also called syntax-awareness, transcodability, or transparency, means that encrypted video syntax in compatible to syntax of compressed video (Macq and Quisquater, 1995). Interpretation of components of video stream such as slice header, block header and frame header requires a standardized syntax structure if standardized coding algorithm is used for compression.

Sensitive video applications require more security than entertainment applications. Economic value of movie decreases exponentially with time (Ainslie et al., 2005). Cost to break algorithm must be greater than licensing fee and the time required to break algorithm must be more than the time data is required to be kept secure. Joint compression and encryption algorithms have higher efficiency and lesser computational load as compared to compression independent algorithms. Puzzle algorithm is the only lightweight algorithm, which is considered secure. Majority of the video encryption algorithms are insecure for military purposes and can at the best be used for non-sensitive applications, for example business meetings or video on demand.

3.1. Partial encryption

This is a format compliant encryption and reduces encrypted data volumes. The unchanged file format is used to synchronize transmission in error prone wireless networks. Multimedia content is divided into multiple parts, out of which only significant parts are encrypted, keeping others unchanged as shown in Fig. 8.

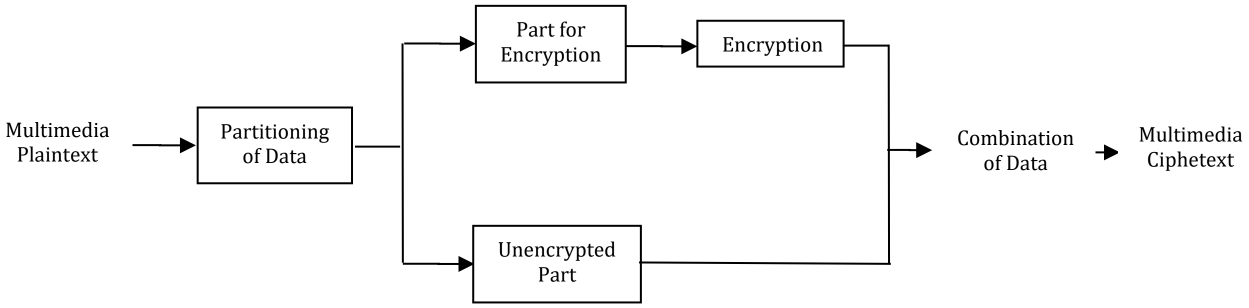

Fig. 8: Partial encryption process (Zhang et al., 2008)

Plaintext can be a region or a block of image, biplane of image pixels, video sequence frame, compressed data stream segment, or a compression codec parameter. Encrypted and non-encrypted parts are combined to create ciphertext media data. Same key or same decryption algorithm is used for decryption of different parts. Plaintext data is partitioned according to blocks, object-background and coding parameters. Data stream is divided in parts, which correspond to coding parameters. Only important parameters are encrypted in parameter passing, keeping the format same. In object-background partitioning, multimedia content is divided into objects and background. Object is encrypted, leaving background unchanged. Block based encoding is appropriate for MPEG and H.263. Data is divided into blocks and only some are encrypted in partial encryption. Layer partitioning encryption scheme is used for progressive encoding. Plaintext is encoded into progressive data streams and only few layers are encrypted in spihit (Said and Pearlman, 1996), ezw (Shapiro, 1993) and MPEG. Encryption based on fractional wavelet transform is more secure because it involves two keys for decryption. It is good for applications where quality degradation is more important than absolute security. Security in partial image encryption is either low or moderate.

Effectiveness of corruption of single bytes of data in MPEG-1 videos can be improved by Huffman encoding. Corruption of single bits may be as efficient as that of bytes, but with increased computational load. Enhanced protection or transparent encryption restricts access to full video to receivers with decryption key; however, base layer can be decoded without key. Transparent encryption does not require any modification at decoder and does not encrypt headers and starting sequences of upper layers. Base layer contains most of the important information and its encryption alone is sufficient to achieve security, while ignoring the enhancement layer. Considering the large bandwidth requirements, partial encryption addresses some of the issues of commercial video security. MPEG-1, MPEG-2, H.261 and H.263 are widely used partial encryption algorithms for video conferencing. Because of use of DCT, they have high potential for dividing data based on relevance. Large amounts of video data are encoded by reference to preceding or following blocks. Thus, only referenced blocks need to be protected. Energy requirement of base layer encryption is comparable to MPEG partial encryption; however, the former has less complexity because it does not need content parsing. MPEG permits different security levels after encoding the data.

Some of the applications of partial audio encryption are wireless multimedia sensor networks, telephone-bandwidth, animal tracking, audio surveillance and human health monitoring. Audio quality, energy efficiency, security and transmission quality are among the goals of the same (Wang et al., 2010). Low-protection scheme is less secure and prevents only common types of attacks, whereas high-protection scheme encrypts about forty five percent of bitstream (Servetti and De Martin, 2002; Datta and Gupta, 2013). Compression followed by frequency selective partial encryption using low pass filters limits the frequency content of audio data, but increases encryption and decryption time (Servetti et al., 2003). Index based selective audio encryption, which is application oriented is not compatible with the standards and is designed for wireless multimedia sensors (Wang et al., 2010).

3.2. Compression combined encryption

This scheme combines encryption operation with compression and implements both simultaneously. Joint encryption and compression results in less computational overhead, since compression can be assumed to be a special case of encryption. Multimedia compression codes can be classified into Discrete Cosine Transform; Wavelet based codec and Fast Fourier Transform. Algorithms can be classified as coefficient encryption algorithm and entropy code based algorithm. Making data hiding algorithms robust to lossy compression is another challenge, since it can possibly result in loss of embedded information. However, maintaining video or image quality after decryption is a challenge. PSNR, Mean Squared Error, Structural Similarity Index Matrix and Normalized correction are some of the parameters for measuring quality. Stream ciphers treat data as bitstreams irrespective of whether compression is applied. A client, which receives packets, decompresses and decrypts in real time to achieve Quality of Service.

Encryption can reduce compression efficiency due to randomness in output, which is one the drawbacks of using both the techniques together. It occurs either due to modification of statistical properties or due to modification of well-designed compression parameters (Zeng et al., 2011). However, in most of the applications, encryption is done either after or during compression because it does not significantly increase overhead. Generally, ciphertext size increases, which is one of the reasons why compression is used. Fig. 9 is screenshot of 720p video used to compare percentage change in ciphertext size as compared to plaintext size. The original video was of 123,431 bytes. Fig. 10 is screenshot of 360p video used to compare change in ciphertext size as compared to plaintext size. The unencrypted video was of 73,387 bytes. Fig. 11 is screenshot of lenna image used to compare increase in ciphertext size as compared to plaintext size. Size of lenna image was of 20,589 bytes. Table 2 compares percentage increase in ciphertext size for various algorithms.

Fig. 9: Screenshot of 720p video used to compare percentage change in file size

Fig. 10: Screenshot of 360p video used to compare percentage change in file size

Fig. 11: Lenna image used to compare percentage change in file size

3.3. Perceptual encryption

It is among the most important reasons for joint encoding and encryption. Some of the applications of perceptual encryption are video on demand and pay-per-view. Ciphertext is degraded but recognizable without decryption, thus it allows untrusted parties to postprocess the encrypted content. It decreases perceivable quality of plaintext by encrypting smallest subset of plaintext but requires syntax compliance for playing (Grgic et al., 2009).

Table 2: Percentage increase in ciphertext size as compared to plaintext size

Cipher	Lenna image	Cat video	720p video
Blowfish	0.1019962115692846	0.0286154223500075	0.0170135541314581
Twofish	0.1019962115692846	0.0286154223500075	0.0170135541314581
Cast	0.1019962115692846	0.0286154223500075	0.0170135541314581
Ice	0.1019962115692846	0.0286154223500075	0.0170135541314581
Mars	0.1019962115692846	0.0286154223500075	0.0170135541314581
Misty	0.1019962115692846	0.02861542235000749	0.01701355413145806
RC2	0.1019962115692846	0.02861542235000749	0.01701355413145806
RC4	0.1019962115692846	0.02861542235000749	0.01701355413145806
RC6	0.1019962115692846	0.02861542235000749	0.01701355413145806
AES	0.1019962115692846	0.02861542235000749	0.01701355413145806
Tea	0.1019962115692846	0.02861542235000749	0.01701355413145806
Tripple DES	0.1019962115692846	0.02861542235000749	0.01701355413145806
Serpent	0.1019962115692846	0.02861542235000749	0.01701355413145806
RSA	28.06838603137597746369420564379	28.022674315614482128987422840558	28.071554147661446476168871677293

It allows users to view and listen low quality version of multimedia before buying. Two parameters that can be used to control the amount of degradation are quality factor and zone of encryption. Zone of encryption does not apply to audio, since it determines visual regions.

First step in perceptual encryption is preprocessing, in which signal partitioning, noise removal, subsampling and color space conversion (Lukac, 2012) are performed. It removes redundancy and prepares plaintext for future steps, for example changing color encoding to separate chrominance and luminance components. Partitioning is another preprocessing methodology, which speeds up the encoding process. Second step i.e. lossy coding follows it, which removes psycho-visually redundant information. It works by converting from spatial to frequency domain using discrete wavelet transform and discrete cosine transform, and quantizing the transform coefficient into integers. Transform decorrelates the original image or video so that correlative information in transform domain is less than spatial domain. Lossy coding is not mandatory because of possible applications in forensics and medical imaging. It is followed by lossless encoding which encodes in compact form, reducing the bits required for same amount of data. Lossless coding methodologies are based on entropy coding since they are based on information entropy. Arithmetic coding and Huffman coding are the most widely used entropy coding mechanisms. Run-length coding and dictionary coding are the most commonly used lossless coding algorithms.

3.4. Video scrambling

It is due to scrambling that an average receiver can view fifty to two hundred channels in television receive only industry. Video scrambling technology such as VB-CSA is used to encrypt video stream. Such kind of video can only be decrypted by authorized users in video service protection system. Video inversion is one the scrambling technique in which polarity of video is reversed. If television can do synchronization of the signal, it produces a negative picture. High lights become dark and dark areas become light. Colours become complementary to the original frame. Sine wave scrambling is a methodology in which a sine wave of 15.75 kHz is added to video signal. Unscrambling is done by taking scrambled signal and adding inverse sine wave of appropriate phase to it. However, it is not much popular nowadays. Transform-based scrambling uses residual coefficient in frequency domain such as DCT or wavelet. DCT based schemes use motion vector scrambling, sign encryption and DCT coefficient scrambling. Wavelet-based mechanism use block shuffling, block rotation and selective bit scrambling. Intra prediction mode scrambling and motion vector scrambling are further examples of scrambling. All these algorithms except intra prediction mode scrambling increase the bit rate. Generally, it takes more computational resources for full scrambling as compared to partial scrambling. Some literature have distinguished between encryption and scrambling (Ibrahim, 2007). The purpose of scrambling is to unevenly distribute stream of 0's and 1's so that more even energy distribution is obtained.

3.5. Other forms of encryption

Selective encryption was introduced to reduce the amount of encrypted MPEG data in video while maintaining appropriate security. Security of AES and RSA are calculated on the basis of difficulty of doing brute force attack. Use of selective encryption depends on how much of plaintext can be kept unencrypted with extremely low probability of a brute force attack. Direct Encryption (Sasaki, 2007) is also called complete encryption and can be further classified as compressed data encryption and raw data encryption. It symmetrically encrypts compressed or raw data directly. Entropy Code Based encryption combines encryption with entropy coding to achieve secures entropy coding. Entropy coding tables are chosen by keys, which slightly reduce compression ratio (Zheng et al., 2006). Coefficient Encryption Algorithm is used during the compression of image or video, wavelet transformation or DCT. The coefficients thus produced in frequency domain are quantized, scanned and encoded. Scalable Encryption is a video codec in which ciphertext consist of a base layer and enhancement layers. Generally multimedia algorithms were not designed for encryption, thus the need for syntax compliant encryption occurs at the decoding side. It is still an active area of research. Syntax compliance also solves the problem of backward compatibility. Such encryption mechanism has advantages such as transparency, scalability, error resilience and adaptability. Transparent Encryption is used in digital TV broadcasting, where low quality content is available to all the users and high quality content is available only for paid users. Low quality video is provided for promotional purposes (Uhl and Pommer, 2004). This type of encryption does not require changes in application program. However, it is not appropriate for applications, which require high security.

Steganography, which is used to hide existence of message, becomes more secure if combined with encryption. Pure steganography does not require prior exchange of secret information. Secret key steganography is considered insecure because it violates Kerckhoff's principle. Decoding algorithm can be used in any cover irrespective of the fact whether it contains secret message. Security depends on the intelligibility of encrypted content. Perceptual attacks on selective encryption can be performed by two methods. First is to assume encrypted parts as loss caused by lost packets or bit errors and use error-concealment to reconstruct plaintext. Second is to replace ciphertext with arbitrary data and determine if visible information can be recognized from rendered content (Wu and Kuo, 2005).

Scalable content is encrypted progressively in layers (Yuan et al., 2003), depending on significance of layers. Insignificant layers are cut off without decryption when cipher text content is transmitted from Internet to bandwidth-limited mobile networks. Table 3 compares throughput in bytes per second for different algorithms. Fig. 12, Fig. 13, and Fig. 14 shows screenshot of videos used for calculating throughput. Fig. 12 is a video of laboratory with file size of 969,740,174 bytes. Fig. 13 is a video of earth taken from satellite with file size of 561,621,821 bytes. Fig. 14 is a video which was taken from a drone. The file size was 1,187,689,257 bytes.

In addition to it, commutative watermarking and encryption, visual cryptography, chaos based encryption and multi-access encryption are the other forms of encryption mechanisms used for multimedia. Signal to noise ratio is one of the quality metrics for quality of encryption. Quality level, which is denoted as QL, describes the quality level of ciphertext image. Unsuccessful encryption is classified as QL2 and is not understandable. In case the shape is intelligible and texture is unclear, it is characterized as QL1. QL0 represents complete encryption. Peak signal to noise ratio can be a possible metric for quality measurement, which measures quality loss by transmission errors, compression and noise. Greater the value of peak signal to noise ratio, better is image quality. Image has three dimensions. First two being width and height and pixel grey level being the third dimension. Pixels have different grey levels, thus value of Fractal dimension ranges from 2 to 3. Greater value of fractal dimension denotes greater randomness and security.

Fig. 12: Screenshot of first video used to compare throughput

Fig. 13: Screenshot of second video used to compare throughput

Fig. 14: Screenshot of third video used to compare throughput

4. Confusion and diffusion in multimedia encryption

Higher confusion and diffusion result in higher security for a cipher. Block ciphers have higher diffusion but are slow and have higher error propagation as compared to stream ciphers. Considering the amount of data to be encrypted in video, these properties can be a disadvantage. Applying either confusion or diffusion without the other makes the cipher insecure. Chaos based encryption has shown advantages in context of complexity, security, speed, computational overhead and computing power (Chen et al., 2004).

DES, RSA and IDEA are not used for image encryption because of high correlation among pixels and difficulty in diffusing and shuffling data. Chaos based encryption does not enhance security against brute force attack. Diffusion makes discretized chaotic map non-invertible and can spread change of each bit of plaintext to ciphertext. Scharinger (1998) proposed a faster method of image encryption using Kolmogorov flow, which ensured good mixing, however it had a disadvantage of key size being dependent on image size (Fridrich and Simard, 2001; Fridrich, 1998). Two-dimensional and three-dimensional chaotic map solved this problem but with higher computational complexity (Lian et al., 2005).

Table 3: Throughput in bytes per second

Algorithm	Throughput for first video	Throughput for second video	Throughput for third video
Blowfish	9,324,424.75	8,775,340.953125	9,578,139.16935483870967741935483870
Twofish	9,795,355.292929292929292929	9,360,363.68333333333	9,980,581.991596638655421848739496
Cast	9,235,620.7047619047619047619047619	8,509,421.53030303030	9,426,105.2142857142857142857142857
Ice	8,896,698.8440366972477064220183486	8,509,421.53030303030	9,206,893.4651162790697674418604651
Mars	9,148,492.2075471698113207547169811	8,382,415.2388059701492537313432836	8,997,645.886363636363
Misty 1	8,658,394.4107142857142857142857143	8,259,144.4264705882352941176470588	8,797,698.2
RC2	7,078,395.4306569343065693430656934	6,849,046.5975609756097560975609756	7,198,116.709090909090909
RC4	10,316,384.829787234042553191489362	9,683,134.8448275862068965517241379	10,238,700.49137931034482758620687
RC6	8,736,397.963963963963963963	8,640,335.7076923076923076923076923	10,699,903.21621621621621621621
AES	10,101,460.145833333333333333333333	9,206,915.0983606557377049180327869	9,980,581.99159663865546218487394
Tea	8,815,819.7636363636363636363636363636364	8,259,144.426470588235294176470588	8,863,352.6641791044776119402985075
Serpent	7,517,365.6899224806201550387596899	7,293,789.8831168831168831168831169	7,564,899.7261146496815286624203822
3DES	692,6715.5285714285714285714285714	6,766,527.9638554216867469879518072	6,865,255.8208092485549132947976879

Bit recirculation image encryption did solve the problem of low computational complexity but made it vulnerable to known plaintext attack and chosen plaintext attack. 3D chaotic cat maps had better key sensitivity, resistance to differential and statistical attacks and larger key space but had poor diffusion. Table 4 compares percentage of times most frequently occurring ciphertext part was repeated. Fig. 15 was plaintext figure of 1,172 bytes used in experiments. Most of the area of figure is of blue colour. 01101100 were used as key. It was observed that 00111111 had highest frequency of occurrence in ciphertext.

Fig. 15: Image used to calculate confusion and diffusion

5. Performance and security analysis of hardware implementations

Due to latest developments in personal communication systems, use of encryption in cordless, cellular phones, security products, telemetry, streaming video and Internet has extensively increased in reconfigurable hardware. Distance learning, telecommuting, multiple digital TV, internet access, web hosting, video conferencing, video on demand, interactive video and HDTV are some of the applications of hardware implementations of multimedia encryption. They have high bandwidth requirements for upstream and downstream applications, which are easy to achieve in reconfigurable FPGA devices and traditional ASIC's. Some of the standards for video conferencing by International Telecommunication Union (Jedwab and Mitchell, 1989) are H323, H324 and H310. ETSI has set up GSM as a standard for mobile communications (Fan and Hasan, 2007). IEEE LAN/MAN committee developed 802.11a and 802.11b as standard for wireless LAN. Inclusion of AES and ECC as international standards has increased their use in hardware implementations.

Lightweight encryption and hardware implementations are proposed solutions to achieve balance between efficiency and security. Hardware implementations are difficult to update, more secure and computationally efficient. Generally, hardware implementations have advantage of being faster and difficult to reverse engineer. Reconfigurable computing when combined with FPGA exhibits both fine-grained data manipulation and parallelism (Compton and Hauck, 2002).

Table 4: Percentage of times ciphertext parts were repeated

Cipher	Percentage of times blocks or stream got repeated
Blowfish	38.808139534883720930232558139535
Twofish	35.968660968660968660968660968661
Cast	38.904899135446685878962536023055
Ice	35.55250514756348661633493497529
Mars	36.571428571428571428571429
Misty 1	38.550724637681159420289855072464
RC2	39.329934450109249817916970138383
RC4	35.729847494553376906318082788671
RC6	38.241601143674052894924946390279
AES	37.473079684134960516870064608758
Tea	39.813486370157819225251076040172
Serpent	36.523574947220267417311752287122
3DES	37.306064880112834978843441466855

More than thousand input and input pins in FPGA's also aid in parallelism. Specialized carry-chain circuitry accelerates parity and addition, which are important for bit-level and fine-grained manipulation of image processing and encryption applications. FPGA implementations can be more easily integrated into larger platforms, are easy to debug and have lesser compatibility issues. Table 5 compares characteristics of FPGA and ASIC implementations. Table 6 compares throughput of

ASIC and FPGA implementations on Pentium four processor with clock rate of two gigahertz. AES proved fastest for multimedia in FGPA considering large amount of plaintext. DES proved to be fastest for ASIC implementations but is insecure.

Table 5: Comparison of FPGA and ASIC implementations (Gaj and Chodowiec, 2000)

Parameter	FPGA	ASIC
Algorithm Agility	Yes	No
Temper Resistant	Limited	Strong
Access Control to Keys	Moderate	Strong
Design Cycle	Moderately Long	Long
Design Tools	Moderately Expensive	Very Expensive
Testing	Moderately Expensive	Expensive
Upgrading and Maintaining	Inexpensive	Expensive

Table 6: Performance comparison

Algorithm	ASIC Throughput	FPGA Throughput
AES	7.5 Gbps (Saggese et al., 2003)	25.1 Gbps (Grabbe et al., 2003)
DES	10 Gbps (Wong et al., 1998)	21.3 Gbps (Rudra et al., 2001)
RSA-1024	1.47 ms	6.1 ms (Amanor et al., 2005)
ECC (prime)	190 µs (Savaš et al., 2000)	3600 µs (Savas et al., 2005)
SHA-1	2.006 Gbps (Savas et al., 2005)	0.9 Gbps (Dominikus, 2002).
MD5	2.09 Gbps (Savas et al., 2005)	5.86 Gbps (Joye and Quisquater, 2001)

Different platforms have varying requirements. To implement the algorithm on special hardware, it must be efficient to implement it on customized VLSI. Embedded systems pose challenge in implementation because of low speed of hardware improvements as compared to workstations (Schneier, 1993). VLSI implementations require more area and are costly as compared to FPGA. However, VLSI implementations have more speed. FPGA implementations are more flexible, easy to test and take less time to market. However, they have higher power consumption (Rodríguez-Henríquez et al., 2007). Public key cryptographic algorithms are based on mathematical problems, which are difficult to solve.

The most common primitives in various such types of algorithms are modular addition, subtraction, multiplication and variable length rotations. These primitives make algorithm secure are hard to implement, need more space and are slower. Therefore, those algorithms are not used for encryption of multimedia files, and are limited to other important cryptographic applications like key exchange, digital signature and verification. Many encryption algorithms are iterative in nature. N iterations of the algorithm are carried out by feeding back previous round results. N rounds of the algorithm are replicated and registers are provided between the rounds to control the data flow in a high-speed network. Reconfigurable FPGA logic is better for such design goals due to its high speed and density. Symmetric ciphers contain bit wise logic operators, which are easy to program on FPGA CLB. Modular addition or subtraction are present in Blowfish, Cast, Feal, Ghost, Idea, Wake, RC5, RC6, Tea, Safer, K-64, Twofish, RC4, Seal and Twoprime ciphers. Cast, Madryga, RC5 and RC6 make use of variable length rotations. Blowfish, Cast, Deal, Twoprime, Feal, A5, Idea, Cost, RC4, RC5, Safer, Seal, Twofish, DES, Wake, LOKI97, L0KI91, Rijndael, Misty, Tea, MMB, RC6 and K-64 have bitwise XOR in their structure. Fixed-length rotations are used by Deal, DES, Cast, Feal, Cost, Serpent, RC6 and Twofish ciphers. Cast, Idea, RC6, MMB and Rijndael use modular multiplication. Substitution operation exists in structures of Blowfish, Deal, DES, L0KI91, LOKI97, Twofish and Rijndael ciphers. Deal, DES, Ice, L0KI91 and LOKI97 use permutation operation. Tea and Serpent cipher apply non-circular shift operations to obtain ciphertext.

Hardware implementations of triple data encryption standard show that with reasonable throughput and small area, higher throughput can be obtained. Linear feedback shift register based stream ciphers when implemented in hardware can be used in low power wireless networks. Higher cost of upgrading algorithms is one of the disadvantages of hardware implementations. Wired equivalent privacy, RC4 and improved wired equivalent privacy are the ciphers, which are tested in WLAN. Improved wired equivalent privacy is less secure than RC4, but requires less computational cost. Serpent cipher ran eighteen times faster on Xilinx Virtex XCV1000 as compared to a 200 MHZ Pentium Pro (Elbirt and Paar, 2000). Reconfigurable implementation of sieve to factor number is twenty eight times faster as compared to a 200-MHz UltraSparc workstation. Significant improvements in speed are observed in Elliptic curve Cryptography (Leung et al., 2000) and DES when implemented in hardware.

Zhang et al. (2008) proposed a method of encrypting watermarked audio signal. The watermark is inaudible, robust to distortions and difficult to remove by unauthorized access. It works by embedding a minimum of one echo, which is dependent on frequency or time characteristics. Moreover, amplitude and delay must be relative to audio signal. Saggese et al. (2003) received audio signals in form of pulse code modulation. In next stage, encrypted audio data and audio control information are extracted. It does cryptanalysis by comparing decrypted ciphertext with aperiodically inverted video. Grabbe et al. (2003) created a player for converting decrypted data to analog signals. Wong et al. (1998) added error detection and correction to encryption and decryption along with encrypted session keys.

RSA, RC4, DES, 3DES, IDEA, AES and Blowfish have negligible mean square error when used for encryption of text and audio in Virtex-5 FPGA XC5VLX110TFF136. RSA, RC4 and blowfish have negligible mean square error for grayscale image. DES, 3DES, IDEA and AES have mean square errors of 0.1279, 2.4755, 0.2782 and 0.0135 respectively. Table 7 shows total time of encryption and decryption of various algorithms in increasing order from lowest to highest (Mohamed et al., 2012).

Table 7: Comparison of total time for encryption and decryption for audio and grayscale image in increasing order

Time for audio	Time for greyscale image
RC4	RSA
Blowfish	Blowfish
3DES	AES
IDEA	RC4
AES	IDEA
DES	DES
RSA	3DES

Side channel attacks in the form of timing behavior, electromagnetic radiation and power consumption were successfully performed in FPGA implementations. Power analysis attack measures power consumption of device during encryption at regions where traces of using secret key increases (Kocher et al., 1999). FPGA implementations of ECC (Örs et al., 2003), RSA, AES and DES are broken by such attacks (Standaert et al., 2003; Standaert et al., 2004a; Standaert et al., 2004b).

6. Conclusion

Due to unsolved challenges, multimedia encryption may continue to be a topic of future research. Out of various parameters, security in software implementations is the one, which greatly restricts application range. Side channel attacks can be reduced by effective use of padding. It was found that public key cryptosystems are better suited for key distribution in context of multimedia encryption. New challenges and frontiers will surely open in future due to high definition three dimensional video and audio. After security and performance analysis, it is concluded that combination of public and private key in the form of double encryption is one of the best encryption methodologies. Also, combining two different architectures gives an opportunity to combine speed with functionality.

References

Ainslie A, Drèze X, and Zufryden F (2005). Modeling movie life cycles and market share. Marketing Science, 24(3): 508-517.

Amanor DN, Paar C, Pelzl J, Bunimov V, and Schimmler M (2005). Efficient hardware architectures for modular multiplication on FPGAs. In the International Conference on Field Programmable Logic and Applications, IEEE, Tampere, Finland: 539-542. https://doi.org/10.1109/FPL.2005.1515780

Bellare M, Kilian J, and Rogaway P (1994). The security of cipher block chaining. In the 14th Annual International Cryptology Conference Santa Barbara, Springer Berlin/Heidelberg, California, USA: 341-358. https://doi.org/10.1007/3-540-48658-5_32

Bondanov A (2007). PRESENT: An ultra-lightweight block cipher attack. In: Paillier P and Verbauwhede I (Eds.), Cryptographic hardware and embedded systems (CHES'07): 450-466. Springer-Verlag, Berlin, Germany.

Chen G, Mao Y, and Chui CK (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals, 21(3): 749-761.

Compton K and Hauck S (2002). Reconfigurable computing: a survey of systems and software. ACM Computing Surveys (csuR), 34(2): 171-210.

Datta K and Gupta IS (2013). Partial encryption and watermarking scheme for audio files with controlled degradation of quality. Multimedia Tools and Applications, 64(3): 649-669.

De Canniere CT (2006). Trivium: A stream cipher construction inspired by block cipher design principles. In the International Conference on Information Security, Springer, Samos Island, Greece: 171-186. https://doi.org/10.1007/11836810_13

Delfs H, Knebl H, and Knebl H (2002). Introduction to cryptography. Springer, Berlin, Germany.

Dominikus S (2002). A hardware implementation of MD4-family hash algorithms. In the 9th International Conference on Electronics, Circuits and Systems, IEEE, Dubrovnik, Croatia, 3: 1143-1146. https://doi.org/10.1109/ICECS.2002.1046454

Elbirt AJ and Paar C (2000). An FPGA implementation and performance evaluation of the serpent block cipher. In the 2000 ACM/SIGDA 8th International Symposium on Field Programmable Gate Arrays, ACM, Monterey, California, USA: 33-40. https://doi.org/10.1145/329166.329176

Fan H and Hasan MA (2007). A new approach to subquadratic space complexity parallel multipliers for extended binary fields. IEEE Transactions on Computers, 56(2): 224-233.

Fridrich J (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 8(6): 1259-1284.

Fridrich J and Simard R (1997). Secure image ciphering based on chaos: Final report for AFRL. Rome, New York, USA. Available online at: http://cryptome.org/cartome/chaos-int.htm.

Furht B and Kirovski D (2004). Multimedia security handbook. CRC press, Boca Raton, USA.

Gaj K and Chodowiec P (2000). Hardware performance of the AES finalists-survey and analysis of results. Available online at: http://ece.gmu.edu/crypto/

Grabbe C, Bednara M, Shokrollahi J, and Teich J (2003). A high performance vliw processor for finite field arithmetic. In the International Parallel and Distributed Processin, IEEE, Nice, France. https://doi.org/10.1109/IPDPS.2003.1213351

Gregory P (2015). CISSP guide to security essentials. Cengage Learning, Boston, USA.

Grgic M, Delac K, and Ghanbari M (2009). Recent advances in multimedia signal processing and communications. Springer, Berlin, Germany.

Gunasekera S (2012). Android Apps security. Apress, New York, USA.

Heys HM and Zhang L (2011). Pipelined statistical cipher feedback: A new mode for high-speed self-synchronizing stream encryption. IEEE Transactions on Computers, 60(11): 1581-1595.

Hudde HC (2009). Building stream ciphers from block ciphers and their security. Seminararbeit Ruhr-Universität Bochum. Available online at: http://www.emsec.rub.de/media/crypto/attachments/files/2011/03/hudde.pdf

Ibrahim KF (2007). Newnes guide to television and video technology: The guide for the digital age-from HDTV, DVD and flat-screen technologies to multimedia broadcasting, mobile TV and Blu-Ray. Elsevier Newnes, Amsterdam, Netherlands.

Jedwab J and Mitchell CJ (1989). Minimum weight modified signed-digit representations and fast exponentiation. Electronics Letters, 25(17): 1171-1172.

Joshi JM and Dalal UD (2012). Histogram matching attack on selective perceptual video encryptions in H. 264/AVC. In the Annual IEEE India Conference, IEEE, Kochi, India: 357-360. https://doi.org/10.1109/INDCON.2012.6420643

Joye M and Quisquater JJ (2001). Hessian elliptic curves and side-channel attacks. In Conference of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, London, UK: 402-410. https://doi.org/10.1007/3-540-44709-1_33

Knudsen LR and Robshaw M (2011). The block cipher companion. Springer Science and Business Media, Berlin, Germany.

Kocher P, Jaffe J, and Jun B (1999). Differential power analysis. In the Advances in Cryptology Conference (CRYPTO'99), Springer Berlin/Heidelberg, Heidelberg, Germany: 388-397. https://doi.org/10.1007/3-540-48405-1_25

Leung, KH, Ma KW, Wong WK, and Leong PHW (2000). FPGA implementation of a microcoded elliptic curve cryptographic processor. In the IEEE Symposium on Field-Programmable Custom Computing Machines, IEEE, Napa Valley, USA: 68-76. https://doi.org/10.1109/FPGA.2000.903394

Li S, Chen G, Cheung A, Bhargava B, and Lo KT (2007). On the design of perceptual MPEG-video encryption algorithms. IEEE Transactions on Circuits and Systems for Video Technology, 17(2): 214-223.

Lian S, Sun J, and Wang Z (2005). Security analysis of a chaos-based image encryption algorithm. Physica A: Statistical Mechanics and its Applications, 351(2): 645-661.

Liu F and Koenig H (2005). Puzzle–a novel video encryption algorithm. In: Dittmann J, Katzenbeisser S, and Uhl A (Eds.), Communications and multimedia security: 88-97. Springer Berlin/Heidelberg, Heidelberg, Germany.

Liu F and Koenig H (2010). A survey of video encryption algorithms. Computers and Security, 29(1): 3-15.

Lukac R (2012). Perceptual digital imaging: Methods and applications. CRC Press, Boca Raton, USA.

Macq BM and Quisquater JJ (1995). Cryptology for digital TV broadcasting. Proceedings of the IEEE, 83(6): 944-957. https://doi.org/10.1109/5.387094

Mao Y, Chen G, and Lian S (2004). A novel fast image encryption scheme based on 3D chaotic baker maps. International Journal of Bifurcation and Chaos, 14(10): 3613-3624.

Mohamed MA, Abou-Elsoud ME, and El-din WK (2012). Hardware implementation of multimedia encryption techniques using FPGA. International Journal of Computer Science Issues, 9(3): 290-300.

NIST (2001). Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197 (FIPS 197). National Institute of Standards and Technology, Gaithersburg, USA. Available online at: nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

Örs SB, Oswald E, and Preneel B (2003). Power-analysis attacks on an FPGA-first experimental results. In the 5th International Workshop on Cryptographic Hardware and Embedded, Cologne, Germany, 2779: 35-50. https://doi.org/10.1007/978-3-540-45238-6_4

Paar C and Pelzl J (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science and Business Media, Berlin, Germany.

Pachghare VK (2015). Cryptography and information security. PHI Learning Pvt. Ltd, New Delhi, India.

Rodríguez-Henríquez F, Saqib NA, Perez AD, and Koc CK (2007). Cryptographic algorithms on reconfigurable hardware. Springer Science and Business Media, Berlin, Germany.

Rudra A, Dubey PK, Julta CS, Kumar V, Rao JR, and Rohatgi P (2001). Efficient rijndael encryption implementation with composite field arithmetic. In the 3th International Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 2162: 171-184. https://doi.org/10.1007/3-540-44709-1_16

Saggese GP, Mazzeo A, Mazzocca N, and Strollo AG (2003). An FPGA-based performance analysis of the unrolling, tiling, and pipelining of the AES algorithm. In the 13th International Conference on Field Programmable Logic and Applications, Springer, Berlin: 292-302. https://doi.org/10.1007/978-3-540-45234-8_29

Said A and Pearlman WA (1996). A new, fast, and efficient image codec based on set partitioning in hierarchical trees. IEEE Transactions on Circuits and Systems for Video Technology, 6(3): 243-250.

Sasaki H (2007). Intellectual property protection for multimedia information technology. IGI Global, Hershey, USA.

Savas E, Naseer M, Gutub AA, and Koç ÇK (2005). Efficient unified montgomery inversion with multibit shifting. IEEE Proceeding-Computers and Digital Techniques, 152(4): 489-498.

Savaš E, Tenca AF, and Koç CK (2000). A scalable and unified multiplier architecture for finite fields GF($_p$) and GF(2^m). In the International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg, Germany: 277-292. https://doi.org/10.1007/3-540-44499-8_22

Scharinger J (1998). Fast encryption of image data using chaotic Kolmogorov flows. Journal of Electronic Imaging, 7(2): 318-325.

Schneier B (1993). Description of a new variable-length key, 64-bit block cipher (Blowfish). In the International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg, Germany: 191-204. https://doi.org/10.1007/3-540-58108-1_24

Servetti A and De Martin JC (2002). Perception-based partial encryption of compressed speech. IEEE Transactions on Speech and Audio Processing, 10(8): 637-643.

Servetti A, Testa C, and De Martin JC (2003). Frequency-selective partial encryption of compressed audio. In the IEEE International Conference on Acoustics, Speech, and Signal Processing, IEEE, Hong Kong, China, 5: V-668. https://doi.org/10.1109/ICASSP.2003.1200059

Shapiro JM (1993). Embedded image coding using zerotrees of wavelet coefficients. IEEE Transactions on Signal Processing, 41(12): 3445-3462.

Stallings W (2006). Cryptography and network security: principles and practices. Pearson Education India, India.

Stamp M and Low RM (2007). Applied cryptanalysis: breaking ciphers in the real world. John Wiley and Sons, New Jersey, USA.

Standaert FX, Örs SB, and Preneel B (2004a). Power analysis of an FPGA. In the CHES: International workshop on cryptographic hardware and embedded systems, Springer, Cambridge, USA, 4: 30-44. https://doi.org/10.1007/978-3-540-28632-5_3

Standaert FX, Ors SB, Quisquater JJ, and Preneel B (2004b). Power analysis attacks against FPGA implementations of the DES. In the 14th International Conference on Field Programmable Logic and Applications, Springer, Leuven, Belgium: 84-94. https://doi.org/10.1007/978-3-540-30117-2_11

Standaert FX, tot Oldenzeel LVO, Samyde D, and Quisquater JJ (2003). Power analysis of FPGAs: How practical is the attack?. In the 13th International Conference on Field Programmable Logic and Application, Springer, Lisbon, Portugal, 3: 701-711. https://doi.org/10.1007/978-3-540-45234-8_68

Uhl A and Pommer A (2004). Image and video encryption: From Digital rights management to secured personal communication. Springer Science and Business Media, Berlin, Germany.

Wang H, Hempel M, Peng D, Wang W, Sharif H, and Chen HH (2010). Index-based selective audio encryption for wireless multimedia sensor networks. IEEE Transactions on Multimedia, 12(3): 215-223.

Wen J, Severa M, Zeng W, Luttrell MH, and Jin W (2002). A format-compliant configurable encryption framework for access control of video. IEEE Transactions on Circuits and Systems for Video Technology, 12(6): 545-557.

Wong K, Wark M, and Dawson E (1998). A single-chip FPGA implementation of the data encryption standard (DES) algorithm. In The IEEE Bridge to Global Integration Global Telecommunications Conference, IEEE, Sydney, New South Wales, Australia, 2: 827-832. https://doi.org/10.1109/GLOCOM.1998.776849

Wu CP and Kuo CC (2005). Design of integrated multimedia compression and encryption systems. IEEE Transactions on Multimedia, 7(5): 828-839.

Young S and Aitel D (2003). The hacker's handbook: The strategy behind breaking into and defending networks. CRC Press, Boca Raton, USA.

Yuan C, Zhu BB, Wang Y, Li S, and Zhong Y (2003). Efficient and fully scalable encryption for MPEG-4 FGS. In the International Symposium on Circuits and Systems, IEEE, Bangkok, Thailand. https://doi.org/10.1109/ISCAS.2003.1206050

Zeng W and Lei S (2003). Efficient frequency domain selective scrambling of digital video. IEEE Transaction on Multimedia, 5(1): 118-129.

Zeng W, Yu H, and Lin CY (2011). Multimedia security technologies for digital rights management. Academic Press, Cambridge, USA.

Zhang Y, Zheng J, and Ma M (2008). Handbook of research on wireless security. IGI Global, Hershey, USA.

Zheng N, Jiang X, and Lan X (2006). Advances in machine vision, image processing, and pattern analysis. International Workshop on Intelligent Computing in Pattern Analysis/Synthesis, Springer, China. https://doi.org/10.1007/11821045

Zhu BB, Yuan C, Wang Y, and Li S (2005). Scalable protection for MPEG-4 fine granularity scalability. IEEE Transactions on Multimedia, 7(2): 222-233.