Multimedia Security Handbook

Borko Furht and Darko Kirovski

Published by CRC Press LLC in December 2004
Table of Contents is available online at http://www.crcpress.com/shopping_cart/products/product_contents.asp?id=&parent_id=&sku=2773&pc=

Contents

Chapter 4

Chaos-Based Encryption for Digital Images and Videos

Shujun Li, Guanrong Chen
Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Toon, Hong Kong SAR, China
Xuan Zheng
Department of Electrical and Computer Engineering, University of Virginia, 351 McCormick Road, P.O. Box 400743, Charlottesville, VA 22904-4743, USA

4.1 Introduction

Many digital services, such as pay-TV, confidential video conferencing, medical and military imaging systems, require reliable security in storage and transmission of digital images/videos. As the rapid progress of Internet in the digital world today, the security of digital images/videos has become more and more important. In recent years, more and more consumer electronic services and devices, such as mobile phones and PDA (personal digital assistant), have also started to provide additional functions of saving and exchanging multimedia messages. The prevalence of multimedia technology in our society has promoted digital images and videos to play a more significant role than the traditional dull texts, which demands a serious protection of users' privacy. To fulfill such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties.

From early 1990s, many efforts have been made to investigate specific solutions to image/video encryption. Due to the tight relationship between chaos theory and cryptography, chaotic cryptography has also been extended to design image and video encryption schemes. This chapter focuses on different image/video encryption algorithms based on chaos, and clarifies some experiences, lessons and principles of using chaos to design such encryption schemes. To start, a comprehensive discussion on the state-of-the-art of image/video encryption will first be given as background and motivation for the discussion of the chapter.

The organization of this chapter is as follows. In Sec. 4.2, some preliminaries on image/video encryption are first given. Sec. 4.3 is a comprehensive review on today's image/video encryption technology without using chaos theory. Chaos-based image and video encryption schemes are then surveyed in Sec. 4.4. Some experiences, lessons and principles drawn from existing chaos-based image/video encryption algorithms are commented and discussed in Sec. 4.5. The last section concludes the chapter.

4.2 Image/Video Encryption: Preliminaries

4.2.1 A Brief Introduction to Modern Cryptography

To facilitate the following discussion, in this subsection, we first give a brief introduction to the basic theory of modern cryptography [1].

An encryption system is also called a *cipher*, or a *cryptosystem*. The message for encryption is called *plaintext*, and the encrypted message is called *ciphertext*. Denote the plaintext and the ciphertext by P and C, respectively. The encryption procedure of a cipher can be described as $C = E_{K_e}(P)$, where K_e is the encryption key and $E(\cdot)$ is the encryption function. Similarly, the decryption procedure is $P = D_{K_d}(C)$, where K_d is the decryption key and $D(\cdot)$ is the decryption function. Following Kerckhoffs' principle [1], the security of a cipher should only rely on the decryption key K_d, since adversaries can recover the plaintext from the observed ciphertext once they get K_d.

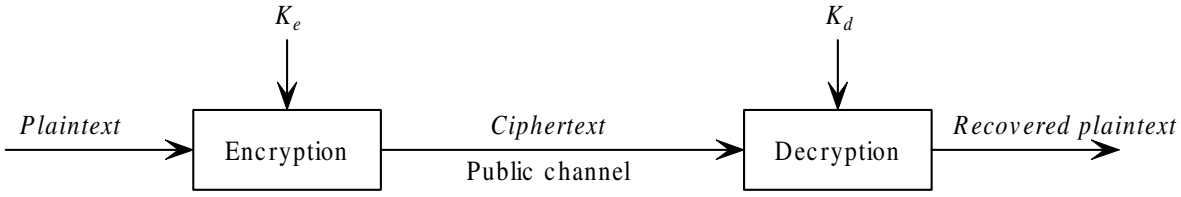


Figure 4.1: Encryption and decryption of a cipher

There are two kinds of ciphers following the relationship of K_e and K_d. When $K_e = K_d$, the cipher is called a *private-key* cipher or a *symmetric* cipher. For private-key ciphers, the encryption-decryption key must be transmitted from the sender to the receiver via a separate secret channel. When $K_e \neq K_d$, the cipher is called a *public-key* cipher or an *asymmetric* cipher. For public-key ciphers, the encryption key K_e is published, and the decryption key K_d is kept private, for which no additional secret channel is needed for key transfer.

According to the encryption structure, ciphers can be divided into two classes: *block ciphers* and *stream ciphers*. Block ciphers encrypt the plaintext block by block, and each block is mapped into another block with the same size. Stream ciphers encrypt the plaintext with a pseudo-random sequence (called *keystream*) controlled by the encryption key.

A cryptographically secure cipher should be strong enough against all kinds of attacks. For most ciphers, the following four attacks should be tested: 1) *ciphertext-only attack* - attackers can get the ciphertexts only; 2) *known-plaintext attack* - attackers can get some plaintexts and the corresponding ciphertexts; 3) *chosen-plaintext attack* - attackers can choose some plaintexts and get the corresponding ciphertexts; 4) *chosen-ciphertext attack* - attackers can choose some ciphertexts and get the corresponding plaintexts. It is known that many image/video encryption schemes are not secure enough against known/chosen-plaintext attack, as further shown below.

4.2.2 The Need for Image/Video Encryption Schemes

The simplest way to encrypt an image or a video is perhaps to consider the 2-D/3-D stream as a 1-D data stream, and then encrypt this 1-D stream with any available cipher [2–5]. Following [6–8], such a simple idea of encryption is called *naive encryption*. Although naive encryption is sufficient to protect digital images and videos in some civil applications, the following issues have to be taken into consideration when advanced encryption algorithms are specially designed for sensitive digital images and videos, for their special features are very different from texts:

1. **Tradeoff between bulky data and slow speed**: Digital images and videos are generally bulky data of large sizes, even if they are efficiently compressed (see discussion below). Since the encryption speed of some traditional ciphers is not sufficiently fast, especially for software implementations, it is difficult to achieve fast and secure real-time encryption simultaneously for large-sized bulky data.

2. **Tradeoff between encryption and compression**: If encryption is applied before compression, the randomness of ciphertexts will dramatically reduce the compression efficiency. Thus, one has to apply encryption after compression, but the special and various image/video structures make it difficult to embed an encryption algorithm into the integrated system. For example, some popular compression standards (such as MPEG-x) are antagonistic to selective encryption [9]. That is, there exist notable tradeoffs between the compression and the encryption [10].

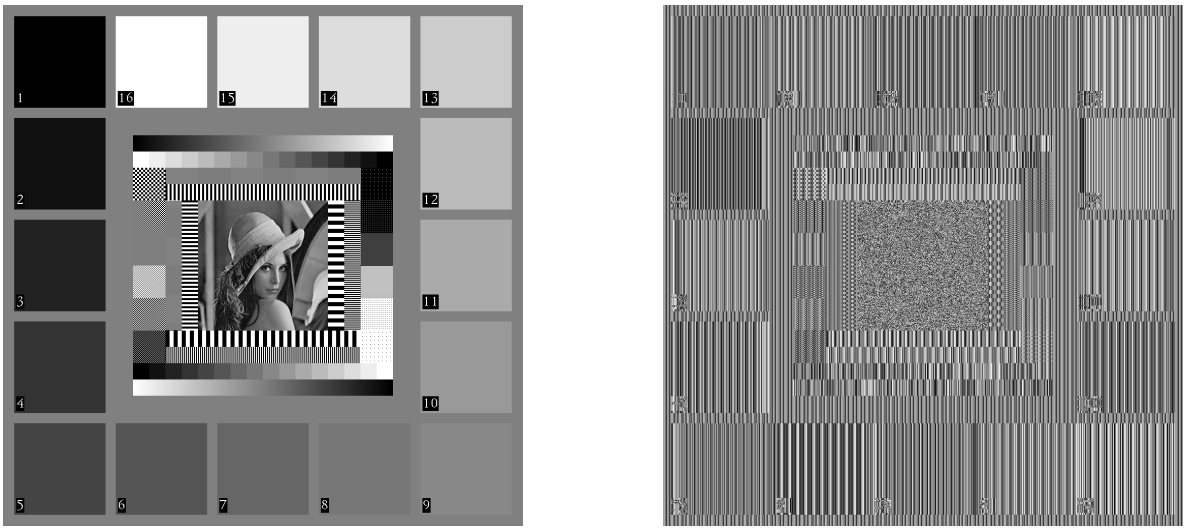
3. **Dependence of encryption on compression**: Lossy compression technique is widely-used for images/videos to dramatically reduce the size of the data for encryption, and it is natural to expect that the design and implementation of fast encryption schemes will be easier. However, it was pointed out [11] that the encryption

cannot benefit much from such a data reduction, since generally the time consumed by the compressor is much longer than that by the encryption algorithm. This implies that the encryption efficiency depends heavily on the involved compression algorithm.

4. **Incapability of compression to reduce data size**: In general, lossy compression of images/videos is not acceptable in some applications due to legal considerations. Medical imaging systems are well-known examples, where the diagnostic images and videos of all patients are required to be stored in lossless forms. In this case, the only choice is to use lossless compression or to leave the images/videos uncompressed, which emphasizes once again the tradeoff between bulky data and slow encryption speed.

5. **Intractable high redundancy**: There exists high (short-distance and long-distance) redundancy in uncompressed images and videos, which may make block ciphers running in ECB (Electronic Code Book) mode fail to conceal all visible information in some plain-images/videos. As a result, block cipher running in CBC (Cipher Block Chaining) mode (or other modes [1]) or stream ciphers should be used to encrypt uncompressed images and videos with high redundancy.

    - If an image contains an area with a fixed color, which means large redundancy, the edge of this area will be approximately preserved after encryption. This is because those consecutive identical pixels lead to the same repeated patterns when a block cipher is used in ECB mode. See Figure 4.2 for a real example of this phenomenon.



a) The plain-image b) The cipher-image

Figure 4.2: An uncompressed plain-image containing many areas with fixed gray-levels and its corresponding cipher-image encrypted by 128-bit AES running in ECB mode

    - Interestingly, a recent work [12] reported that encrypted BMP images (uncompressed) are less random than encrypted JPEG images (compressed), which implies that the high redundancy cannot be efficiently removed after encryption.

6. **Loss of the avalanche property**: Apparently, a direct use of traditional ciphers in image and video encryption cannot provide avalanche property at the level of image and video frame. For example, for two images with only one bit difference at the position (i, j), all cipher-pixels except for the ones at (i, j) will be identical in ECB mode, and all cipher-pixels before (i, j) will be identical in CBC mode. To maintain the avalanche property, special algorithms should be developed.

7. **New concepts of security and usability**: The diverse multimedia services need different security levels and usability requirements, some of which should be defined and evaluated with human vision capabilities. A typical example is the so-called perceptual encryption, with which only partial visible information is encrypted and the cipher-image/video gives a rough view of the high-quality services.

4.2.3 Some Special Features of Image/Video Encryption Schemes

In image/video encryption systems, some features are required to support special functions of diverse multimedia services in different environments. These features are generally realized with a combination of compression and encryption, and impose some limits on the design of the image/video encryption algorithms.

- **Format-compliance** (also called *syntax-awareness* [13], *transcodability* [14] or *transparency*): This feature means that the encrypted image/video is still decodable at the receiver end without the knowledge about the decryption key. For online stream multimedia services, especially those running in wireless environments, the transparency property is desirable to eliminate the problems caused by loss or uncorrected data. Transparency property is also useful to ease concatenating other postprocessing devices (such as digital watermarking) to the whole compression/encryption system errors [13, 15]. To achieve transparency, the encryption procedure should not destroy the syntax structure of the encrypted file/stream; that is, the descriptive information of the file/stream should be left unencrypted.
- **Scalability**: Scalability means multi-level security for different applications with flexible parameter settings [16–25]. The embedded multi-layer structure, i.e., the fine granularity scalability (FGS), of JPEG2000 images [26] and MPEG-2/4 videos [27] makes scalable encryption easy and natural. The basic idea to realize scalability is to encrypt partial layers and/or partial data in selected layers. Scalability can be considered as a control mechanism for the visual quality of the encrypted image/video.
- **Perceptibility**: Perceptibility means partial encryption of visible information of the plain-image/video, which is useful for pay-after-trial services of digital multimedia, such as pay-TV and VoD services [14]. It is a generalization of scalable (multi-layered) encryption, and does not depend on the embedded multi-layered structure of the encrypted image/video. Two typical perceptual encryption schemes for JPEG images and MP3 music were proposed in [28] and [29], respectively. The selective image encryption schemes proposed in [30–35] and video scrambling schemes in [36, 37] are also examples of perceptibility, although this term was not explicitly used therein.
- **Error-tolerability**: The concept of *error-tolerating* (or *error-resilient*) encryption was investigated in [22, 38] and also mentioned in [13, 15]. It is undesirable if an encrypted stream cannot be decoded when some bit errors are introduced, which frequently occurs in multimedia applications particularly in wireless environments (error-correction mechanism may fail in some situations). However, the avalanche property of good ciphers means high sensitivity to errors, which may lead decryption to fail in some cases. To solve this problem, the idea of selective encryption was used in [22] to provide better error-tolerating property; and, in [38], the possibility to design an *error-preserving* encryption algorithm was studied.

Generally speaking, there exist tight relationships among the above-discussed features: 1) transparency and the idea of *selective encryption* (see below for more details) are requirements of scalability and perceptibility; 2) multi-level security is achieved by providing perceptibility in some scalable encryption schemes.

4.3 Image/Video Encryption: A Comprehensive Survey

Generally speaking, there are two basic ways to encrypt digital images: in spatial domain or in transform domain. Because digital videos are generally compressed in DCT (discrete cosine transform) domain, almost all video encryption algorithms work in DCT domain. Due to the recent prevalence of wavelet compression technique and the adoption of wavelet transform in JPEG2000 standard [26], in recent years image/video encryption algorithms working in wavelet domain also attract some attention [35, 39–43]. In addition, some novel image/video compression algorithms have also been proposed to realize joint compression-encryption schemes.

Although many efforts have been devoted to better solutions for image and video encryption, the current security analyses of many schemes are not sufficient, especially on the security against known/chosen-plaintext attack. What's worse, many selective encryption schemes are indeed insecure against ciphertext-only attack, due to the visible information leaking from unencrypted data.

In this section, we provide a comprehensive survey on image and video encryption schemes without using chaos theory, as a background of chaos-based encryption schemes. Before that, a widely-used idea in the image/video encryption community, called selective (or partial) encryption, is firstly introduced so as to facilitate the security evaluations of selective image/video encryption schemes to be carried out later.

4.3.1 Selective Encryption

Since the 1990s, selective encryption has been widely suggested and adopted as a basic idea for encryption of digital images and videos, aiming to achieve a better tradeoff between the encryption load and the security level. In [22], it was pointed out that selective encryption is also useful for realizing error-tolerating property in wireless video transmission. The MPEG-4 IPMP (Intellectual Property Management and Protection) extensions standard also starts to support selective encryption [44]. In addition, as mentioned above, scalability and perceptibility are generally realized via selective encryption.

Some reviews of selective encryption methods and their performances can be found in [9,45–47], among which [47] gave a partial list of some representative selective encryption methods and [9] analyzed the potential insecurity of different selective syntactic elements in MPEG-2 video stream against possible attacks. Although it seems that selective encryption is a good idea for the design of high-efficiency image/video encryption schemes, some essential defects of selective encryption have been pointed out, showing its incapability to provide a satisfactory balance between security and usability. For selective encryption methods of MPEG videos, for instance, the following defects have been clarified [9–11, 13, 47–50]:

1. Although the energy of a compressed image concentrates on lower DCT coefficients, the visible information does not concentrate on partial coefficients, but scatters over all DCT coefficients. Actually, only one DCT coefficient is enough to recover some visible information of the concerned plain-frame, as shown in Figure 2d of [10] and Figure 5.2 of [51] on some experimental images. By setting all encrypted DCT coefficients to fixed values, it is possible for an attacker to recover a rough view of the plain-frame. A more detailed discussion on this defect can be found in Sec. IV of [13], where this defect is used to realize the so-called *error-concealment attack* (also called *perceptual attack* [9]).

2. The scattering effect of visible information also exists in different bits of DCT coefficients, which makes it insecure to partially encrypt significant bits of DCT coefficients. In Figure 3 of [10], it was shown that neither encrypting the sign bits nor encrypting multiple significant bits are secure enough against ciphertext-only attack utilizing the unencrypted bits.

3. Only encrypting I-frames of a video cannot provide sufficient security against ciphertext-only attack. The unencrypted I-blocks and motion vectors in B and P frames can be still used to uncover partial visible information of the original videos.

4. Because all I-frames occupy about 30%∼60% or even more of an MPEG video [8, 52], the reduction of computation load of encrypting I-frames only is not significant. If all I-macroblocks in B and P frames are also encrypted, the encryption load will be close to that of full encryption. In [11], it was further pointed out that selective encryption of compressed images/videos cannot significantly save the overall processing time, since the compression procedure generally consumes more time than the encryption of the compressed images/videos.

5. If the selective encryption is exerted before the entropy-coding stage, the compression performance will decrease. While if the selective encryption is exerted after the entropy-coding stage, the format-compliance may be lost. If the entropy-coding algorithm is kept secret, the secret entropy codec is generally insecure against plaintext attack, since the sizes of the Huffman tables are too small from the cryptographical point of view.

Apparently, the first two defects of selective encryption of MPEG videos are due to the orthogonality of DCT. Since all transforms used in image/video compression algorithms have the orthogonal property, the two defects exist for all transform-based image and video compression algorithms. The first two defects on uncompressed images were also pointed out in [50], and the second defect was used in [33] to achieve perceptual encryption with controllable quality of cipher-images.

In [9], a comparison of the performances of selectively encrypting different syntactic elements of MPEG-2 was given, and three kinds of relationships between the compressor and the selective encryption system were clarified: cooperative, neutral, and antagonistic. Although it was thought in [9] that the relationship between the MPEG compressor and almost selective MPEG encryption schemes is neutral, the aforementioned defects of selective MPEG encryption imply that the MPEG compressor plays an antagonistic role with respect to the selective encryption.

As a summary, considering the security defects of selective image/video encryption, it is difficult to simply use the idea of selective encryption alone to achieve a high security level. From a conservative point of view,

the meaningful use of selective encryption is to realize perceptual encryption, i.e., to degrade the visible quality of the encrypted plain-image/video, rather than to provide cryptographically strong security. It has been argued that selective encryption can work well with model-based compression algorithms, such as context-based arithmetic coding [53] and model-based speech coding [10], but further studies are still needed to confirm the security level of the selective encryption in such compression models.

4.3.2 Joint Image/Video Encryption Schemes

Due to the similarity between MPEG videos and JPEG images, most MPEG encryption methods can be used to encrypt JPEG images directly [33, 54, 55]. On the other hand, some encryption techniques proposed for images can also be extended to encrypt videos with similar structures. Therefore, the distinction between image encryption and video encryption is not prominent. In this subsection, we discuss those schemes lying on their boundary: the joint image/video encryption schemes.

- Almost all *DCT-based encryption schemes* can be used to encrypt both JPEG images and MPEG videos, although most DCT-based encryption schemes were originally proposed for MPEG videos, with a few for JPEG images [33, 55]. Video encryption schemes for MPEG will be further discussed in Sec. 4.3.4.

- Because entropy coding is widely used in image/video compression algorithms, the idea of *making entropy codec secret* can work for both image and video encryptions.

  - In [56, 57], the secretly-permuted Huffman table is used to encrypt the input image/video stream. This scheme is not secure enough against known/chosen-plaintext attacks, and its key space is too small.
  - In [10], multiple Huffman tables (MHT) are employed and a random index is used as the secret key to select a Huffman table for each codeword. This scheme cannot resist the chosen-plaintext attack. Later, two methods were proposed to enhance its security: secretly inserting pseudo-random bits [58] and changing the random index frequently [58, 59].
  - In [60], another encryption scheme based on secret Huffman tables was proposed. Random flipping of the last bit of each codeword is introduced to further adaptively change the Huffman table.
  - In [13, 15], the Huffman tables are left untouched and the secret entropy codec is achieved as follows: map each plain-codeword to an index representing its position in the Huffman table, encrypt the index, and then re-map the encrypted index back to generate cipher-codeword.

- All *wavelet-based* image *encryption schemes* can be extended to encrypt videos based on wavelet compression algorithms, such as motion JPEG2000 [26]. Wavelet-based image encryption schemes will be surveyed in the next subsection.

  - In [61, 62], it was suggested to use the following three operations for encryption of wavelet-compressed videos: selective bit scrambling, block shuffling, and block rotation. It appears that this scheme cannot resist the chosen-plaintext attack.
  - In [51, 63, 64], the use of selective encryption in SPIHT encoded images was studied, in which SPIHT coding is cooperative with the selective encryption.

- In [51, 63–65], the use of selective encryption in *quadtree decomposition* of digital images was discussed in detail. It was pointed out that Leaf Ordering I (from top to bottom) is not sufficiently secure in the selective encryption framework. This scheme was also extended to selective video encryption.

- In [53], a selective encryption scheme based on *context-based arithmetic coding of DWT* (discrete wavelet transform) coefficients, was proposed. This scheme uses a traditional cipher to selectively encrypt partial leading bits of the compressed bitstream. Without the knowledge of the leading bits, it is cryptographically difficult to decompress the bitstream due to the sensitivity of the decompression to the leading bits (i.e., to the modelling context). This scheme is a good example that exhibits the cooperative relationship between compression and selective encryption.

4.3.3 Image Encryption Schemes

- One of the simplest idea to selectively encrypt images in the spatial domain is to *encrypt one or more bit-planes* [33,66,67]. Since the MSB (most significant bit) contains the most defining information on the image, it serves as the first bit-plane for encryption. As a result, the selection order is generally from MSB to LSB [66,67], but the order should be reversed for perceptual encryption schemes so as to reserve some visible information [33].

- In [68], a *VQ-based image encryption* algorithm was proposed. In this scheme, the codebook is first extended, then transformed to another coordinate system, and finally permuted to make a shuffled codebook in a larger size. The parameters used in the above three processes are encrypted with a traditional cipher. It was claimed [68] that this scheme can resist all kinds of known attacks, and the encryption load is very light.

- In [39], *secret permutations* were suggested to shuffle the *DWT coefficients* in each subband of wavelet compressed images. An enhanced version of this scheme suggested encrypting the lowest subband with a traditional cipher. In [69], some permutation methods of DWT coefficients were compared, and a novel method was proposed to realize stronger confusion of shuffled coefficients. Because of the scattering effect of visible information in all DWT coefficients (see Figures 1 and 3 of [39]), such permutations alone are not secure enough against the ciphertext-only attack, if not all subbands are permuted. Also, the secret permutations can be reconstructed under known/chosen-plaintext attacks.

- In [32,35], several perceptual encryption schemes were proposed by *selectively encrypting partial DWT coefficients*. The bit-shift encryption function used in [35] is not secure enough against known/chosen-plaintext attacks. In [67, 70], the use of selective encryption in JPEG2000 image encryption was discussed. It was pointed out that at least 20% of encrypted data are needed to provide sufficient security.

- In [43], *encryption of sign bits of partial DWT coefficients* was suggested. This scheme is not secure due to the aforementioned second defect of selective encryption.

- In [71], the idea of *encrypting wavelet filters* was proposed to develop a new encryption system. Later, in [40, 41, 72], this algorithm was studied with wavelet packet decomposition, and it was shown that such an encryption scheme is not secure enough against the ciphertext-only attack based on a heuristic cryptanalytic method.

- In [41, 42, 73, 74], the possibility of *encrypting the quadtree decomposition structure* was studied for images compressed with *wavelet packet algorithms*. Uniform scalar quantization of wavelet coefficients was found insecure against the ciphertext-only attack, and the zero-tree coder was suggested to provide higher security.

- *Encryption schemes based on fractal compression* were proposed in [30,31]. Selected parameters are encrypted to achieve perceptibility.

- In [75], an image encryption scheme was proposed based on the so-called *base-switching lossless compression algorithm*. The base-switching compression is a simple lossless algorithm, which compresses each 3×3 block of the image into a 3-tuple data (m, b) and an integer with 9 b-base bits. The base b of each block is encrypted with a secret polynomial function to generate the cipher-image. Apparently, this scheme cannot resist known/chosen-plaintext attacks, since using a polynomial function is not sufficiently secure from the cryptographical point of view.

4.3.4 Video Encryption Schemes

MPEG encryption schemes

- The most frequently used idea of MPEG encryption is to *encrypt selective frames, macroblocks, DCT coefficients and/or motion vectors*. The following is a list of selective data for encryption in different schemes (from light to heavy encryptions):

  - All header information (and partial blocks) [76].
  - Selective AC coefficients of Y/V blocks in all I-frames [77].

  - Selective leading DCT coefficients of each block [78].
  - Selective DCT coefficients of each block and motion vectors [61, 62].
  - All or selective motion vectors [36].
  - All I-frames [34, 79] and the header of the MPEG video sequence [48, 80].
  - All I and P frames [79], or all I-frames and I-macroblocks in B and P frames [76].
  - All or selective I-macroblocks and the headers of all predicted macroblocks [81].

  Note that almost all selective MPEG encryption schemes have the defects mentioned in Sec. 4.3.1, and the encryption of the headers will cause the loss of format compliance.

- Another frequently used idea is to *secretly permute all or selective macroblocks, blocks, DCT coefficients and/or motion vectors*.

  - In [54], DCT coefficients are secretly permuted within each block, and the DC coefficient is split into two halves and the 63rd AC coefficient is set to be the higher half of the DC coefficient.
  - In [61, 62], the following three operations are combined to encrypt images: secret permutations of DCT coefficients, selective encryption of DCT coefficients, and motion vector scrambling. In this scheme, several blocks compose a segment, and DCT coefficients in different blocks at the same frequency are secretly permuted.
  - In [82], the secret permutations of DCT coefficients and the encryption of sign bits of DC coefficients are combined to realize a selective encryption scheme.
  - In [13,83], different basic units are secretly permuted: macroblocks, 8×8 blocks, and run-level codewords. The secret permutation tables are pseudo-randomly generated from some encrypted local-content-specific bits.

  The first three schemes above are all insecure against ciphertext-only attack [6,7,49,84,85] and known/chosen-plaintext attacks [6,7,49,84]. Another disadvantage of secret permutation of DCT coefficients is the expansion of the video size [61, 62].

- In [57, 86–88], three encryption schemes were proposed that *encrypt selective sign bits of DCT coefficients and motion vectors*, which are respectively called VEA (video encryption algorithm) [87], MVEA (modified VEA) [86], and RVEA (real-time VEA) [88]. Note that the encryption of sign bits was also involved in other designs [13, 82].

  - VEA is a simple cipher XORing all sign bits with a repeated m-bit key. It is too simple to resist ciphertext-only attack and known/chosen plaintext attacks.
  - MVEA is a simple modification of VEA, in which only sign bits of DC coefficients in I-frames and sign bits of motion vectors in B and P frames are XORed with the secret key. In fact, MVEA is weaker than VEA [57, Appendix].
  - RVEA is a combined version of VEA and MVEA, where the XOR operations are replaced by a traditional cipher. For each macroblock, at most 64 sign bits are encrypted with the order from low frequency to high frequency (see Figure 5 of [57]). Although RVEA is the strongest VEA cipher, the attempt of using unencrypted AC coefficients to reconstruct some visible information is still possible.

Generic video encryption schemes

- In [6,7,52], *another VEA* was proposed to encrypt video stream: divide each 128-byte piece of the plain-video into two 64-byte lists: an Odd List and an Even List, and the Even list is XORed by the Odd list and then encrypted. This VEA can reduce the encryption load by 50%. An extended VEA with lighter encryption cost was proposed in [22] to support the error-tolerability property.

- In [89], a simple video encryption scheme was proposed, which applies a *secret linear transformation* on each pixel value. All pixels in the same macroblock are encrypted with the same secret parameters set. In [37], a similar encryption scheme was proposed. Both schemes are insecure against known/chosen-plaintext attacks.

- In [90], *combining a fast (stream) cipher and a secure (block) cipher* was suggested to achieve overall fast encryption of digital videos. The encryption procedure can be described as follows. Assume that C, M respectively mean the ciphertext and the plaintext, and that $\boldsymbol{SE}, \boldsymbol{FE}$ respectively mean the secure cipher and the fast cipher,

$$C = \{\boldsymbol{SE}(K, M_{ik+1}), \boldsymbol{FE}(K_{i+1}, M_{ik+2}M_{ik+2}\cdots M_{(i+1)k})\}_{i=0}^{t},$$

where $K_{i+1} = \boldsymbol{SE}(K, \boldsymbol{SE}(K, M_{ik+1}))$. Two ciphers with high encryption speeds were designed. Since partial plaintexts are selected to be encrypted with a securer cipher but others are selected to be encrypted by a faster cipher, such a mechanism can be regarded as a generalized version of selective encryption.

4.4 Chaos-Based Image/Video Encryption

Due to the tight relationship between chaos and cryptography, in the past two decades it is widely investigated how to use chaotic maps to construct cryptosystems. For a comprehensive survey of digital chaos ciphers, see Chap. 2 of [91]. Basically, there are two typical ways using chaos in image/video encryption schemes: 1) use chaos as a source to generate pseudo-random bits with desired statistical properties to realize secret encryption operations; 2) use 2-D chaotic maps (or fractal-like curves) to realize secret permutations of digital images/frames. The first way has been widely used to design chaotic stream ciphers, while the second is specially employed by chaos-based image encryption schemes.

4.4.1 Image Encryption Schemes Based on 2-D Chaotic Maps

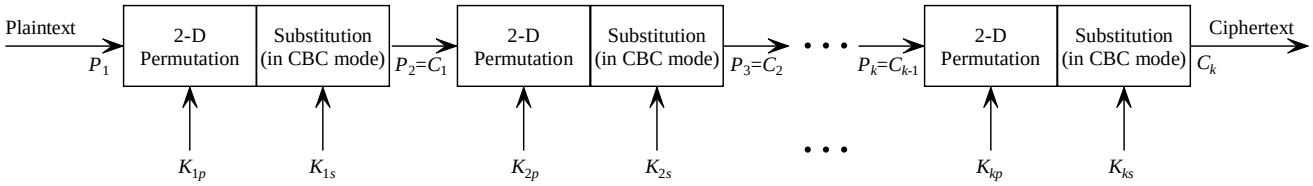


Figure 4.3: A general framework of image encryption systems based on 2-D chaotic permutations (substitution part is run in CBC mode to resist chosen-plaintext attack)

The idea of using 2-D chaotic maps to design permutation-based image encryption schemes was initially proposed in [92–95], and later systematized in [96–98]. Assuming that the size of the plain-image is $M \times N$, the encryption procedure can be described as follows (see Figure 4.3):

- define a discretized and invertible 2-D chaotic map on an $M \times N$ lattice, where the discretized parameters serve as the secret key;
- iterate the discretized 2-D chaotic maps on the plain-image to permute all pixels;
- use a substitution algorithm (cipher) so as to modify the values of all pixels to flatten the histogram of the image, i.e., to enable the confusion property;
- repeat the permutation and the substitution for k rounds to generate the cipher-image.

To resist the chosen-plaintext attack, the substitution part should be used in context-sensitive modes (generally in CBC mode). This is to provide the needed diffusion property for the cipher-image with respect to small changes in the plain-image. The most favorable 2-D chaotic map for discretization is the Baker map whose continuous form is defined as follows:

$$B(x,y) = \begin{cases} (2x, y/2), & 0 \le x < 1/2, \\ (2x-1, y/2+1/2), & 1/2 \le x < 1. \end{cases}$$

It is also possible to use the Cat map and the Standard map as discussed in [97, 98], but it was found that these two maps are not as good as the Baker map.

In [99], it was pointed out that there exist some weak keys in Fridrich's image encryption scheme [96–98]. This problem is caused by the short recurrent-period effect of the discretized Baker map: for some keys, the recurrent-period of the chaotic permutation is only 4. Although this issue was discussed from a statistical point of view, in Sec. 5 of [98] and Sec. 4.2 of [97], the existence of such a short period was not noticed. To overcome this defect, in [100], a modified Fridrich's image encryption scheme was proposed. An extra permutation (shifting pixels in each row) is introduced to avoid short recurrent period of the discretized chaotic permutation. The existence of weak keys signifies the importance of the dynamical properties of the discretized chaotic permutations. However, till now only limited results on a subset of all chaotic possible permutations have been reported [101], therefore further theoretical research is needed to clarify this issue and its negative effect on the security of the image encryption schemes.

Recently, 2-D discretized chaotic maps were generalized to 3-D counterparts: 3-D Baker map in [102–104] and 3-D Cat map in [105]. Based on the proposed 3-D discretized chaotic maps, after re-arranging the 2-D plain-image into a 3-D lattice (over which the 3-D chaotic map is iterated), the plain-image can be encrypted in a similar procedure to the original Fridrich's scheme. Another difference of the two schemes from the Fridrich's scheme is that a chaotic PRNG (pseudo-random number generator) based on the 1-D Logistic map is used to realize the substitution algorithm.

In [106,107], a different discretized rule for the Baker map was proposed and a generalized version of the original Scharinger-Fridrich image encryption schemes [92–98] was developed. For a $2^l \times 2^l$ image, the new discretized Baker map was controlled by a 2^{2l-1}-size sequence $\left\{b_k^{(1)}, \cdots, b_k^{(2^{2l-1})}\right\}$, which determines 2^{2l-1} rotation directions of local pixels. Let the encryption key be of 2^{2l-1} addresses $\left\{a_0^{(1)}, \cdots, a_0^{(2^{2l-1})}\right\}$. The encryption procedure is realized by running the following two combined operations for n times:

1. use selected bits from the pixel values indexed by the 2^{2l-1} addresses to generate $\left\{b_k^{(1)}, \cdots, b_k^{(2^{2l-1})}\right\}$, so as to control the secret permutations;

2. use selected bits from the Y-coordinates of the permuted pixels in the last round to substitute the pixel values in the current round.

The above two operations are similar to those used in the original Scharinger-Fridrich schemes. This generalized encryption scheme has two special features: 1) the decryption key is different from the encryption key; 2) the decryption key depends on both the encryption key and the plain-image. In fact, the decryption key is a permutation of the addresses containing in the encryption key. A defect of this scheme is that its key size is too long.

4.4.2 Image Encryption Schemes Based on Fractal-Like Curves

The permutations defined by discretized 2-D chaotic maps can also be generated from a large group of fractal-like curves, such as the Peano-Hilbert curves [108]. Due to the tight relationship between chaos and fractals, permutation encryption schemes based on fractal-like curves can be designed, which are further discussed in this subsection.

This basic idea of using fractal-like curves to generate noise-like images can be retrospected to early work in image-understanding on noise-like coding of associate memories [109]. In such noise-like associative memories, associative keys are used to store and retrieve data, and the keys can be generated in a way similar to image encryption. For example, in [108], the Peano-Hilbert curve is used to permute all pixels and a pseudo-random mechanism is used to substitute the gray values. In [110], the idea of using chaos to generate keys for noise-like coding memories was also suggested.

In [111], a simple video scrambling scheme was proposed, which encrypts images or uncompressed video frames by scanning all pixels with a secret space-filling curve (SFC). Although it is called a video scrambling method, it actually is an image scrambling algorithm. This scheme can be broken under ciphertext-only attack, as reported in [112]. In addition, it is insecure against known/chosen-plaintext attacks, since the secret permutation can be reconstructed easily with some pairs of plain-images and cipher-images.

Since the 1990s, a number of image/video encryption schemes based on SCAN, which is a fractal-based image processing language [113], have been proposed [114–121] and realized in hardware [122–124]. All SCAN-based image/video encryption schemes can be divided into two generations: the first generation uses secret permutations to encrypt plain-images; the second combines secret permutations and the substitution algorithm. It has been pointed out that the first generation is not secure enough against knwon/chosen-plaintext attacks [51, 64, 125, 126],

and the second can enhance the security of the first generation. In all SCAN-based encryption schemes, the secret permutations are generated from 13 different SCAN patterns and 24 different partition patterns, where the SCAN words serve as the secret key. Figures 1 to 3 of [121] illustrate details about how these SCAN patterns are combined to generate a secret permutation (or a scan order) of the image. In the following, a brief introduction is given to all SCAN-based image/video encryption schemes.

- **The first generation** [114–119]:
  - In [114–116], SCAN language was used to design a SCAN transposition cipher (STC), which is then combined with a stream cipher to compose a product cipher. Following the analyses given in [51,64,125], STC is insecure against known/chosen-plaintext attacks and its security is ensured by another stream cipher.
  - In [117], the SCAN language is combined with quadtree decomposition to encrypt images, where the SCAN language is used to permute the order of four nodes in each level of the quadtree structure. This scheme was insecure due to many security weaknesses, which were discussed in detail in [51].
  - In [118], the SCAN language is slightly modified and then combined with the 2DRE (two-dimensional run-encoding) technique to encrypt binary images. It was pointed out that this cryptosystem cannot resist the known-plaintext attack [126].
  - In [119], the SCAN language is used to compress the image into a shorter binary string, then re-arrange the compressed string into multiple $2^n \times 2^n$ blocks, and finally permute each $2^n \times 2^n$ block with two different SCAN patterns for m times. Apparently, this scheme corresponds to a single STC, which is insecure against known/chosen-plaintext attacks [51, 64, 125].
- **The second generation** [120, 121]: The following substitution mechanism is exerted after permutation, so as to resist known/chosen-plaintext attacks (just like those image encryption schemes based on 2-D chaotic maps):

$$C[j] = (B[j] + (C[j-1] + 1) \cdot R[j]) \bmod 256,$$

  where $R[j]$ is a pseudo-random integer between 0 and 255. Apparently, the substitution algorithm corresponds to a stream cipher with ciphertext feedback. The mixing of different SCAN patterns (two secret SCAN patterns, and two public SCAN patterns – the sprial pattern $s0$ and the diagonal pattern $d0$) and the substitution part makes the new SCAN-based encryption scheme much securer to known/chosen-plaintext attacks.

4.4.3 Image Encryption Schemes Based on 1-D Chaotic Maps

All chaos-based cryptosystems using 1-D chaotic maps can be used to encrypt digital images. It is common to use images to show visible performances of the designed cryptosystems [127–130]. In this subsection, discussion is focused on the chaos-based encryption algorithms specially designed for digital images.

Yen et al.'s image encryption schemes

Yen et al. [131–147] proposed a series of chaos-based image/video encryption schemes. In these proposed algorithms, the employed chaotic map is the Logistic map $f(x) = \mu x(1-x)$ realized in finite computing precision, and the secret key always includes the initial condition $x(0)$ and the control parameter μ (for some schemes, the secret key includes some additional parameters). All these encryption schemes follow a similar basic idea of using chaos to realize encryption:

- run the Logistic map to generate a pseudo-random binary sequence $\{b(i)\}$ from the n-bit representation of each chaotic state $x(k) = 0.b(n \cdot k)b(n \cdot k+1) \cdots b(n \cdot k+n-1)$, where n may be less than the finite computing precision;
- use the chaotic binary sequence $\{b(i)\}$ to pseudo-randomly control permutations and/or value substitutions of all pixels.

Note that the generated sequence $\{b(i)\}$ is generally not balanced, i.e., the number of 0's is different from that of 1's, since the variant density function of the Logistic map is not uniform [148]. That is, the Logistic map is not a good choice for encryption, so it is better to use other 1-D chaotic maps with uniform variant density instead. However, in the following, once can see that Yen et al.'s encryption schemes are not secure even when $\{b(i)\}$ satisfies the balance property.

- **BRIE** (*Bit Recirculation Image Encryption*) [137]: $\{b(i)\}$ is used to pseudo-randomly control shift operations exerted on each pixel. This scheme has been cryptanalyzed in [149]. Due to the essential defects of rotation shift operations, the encryption performance of this scheme is rather poor when some specific secret keys are used. Also, it cannot resist known/chosen-plaintext attacks, since a mask image that is equivalent to the secret key can be derived from a pair of plain-image and cipher-image.

- **CKBA** (*Chaotic Key-Based Algorithm*) [138]: $\{b(i)\}$ is used to pseudo-randomly XOR (or NXOR) each pixel with $key1$ or $key2$, where $key1, key2$ are also included in the secret key. According to [150], CKBA cannot resist known/chosen-plaintext attacks. Only one pair of known/chosen plain-image and cipher-image is enough to reconstruct $key1, key2$ and then derive $\{b(i)\}$. From $\{b(i)\}$, $x(0)$ and an approximate value of μ can also be found.

- **HCIE** (*Hierarchical Chaotic Image Encryption*) [131, 133, 139]: In this scheme, an $M \times N$ plain-image is divided into $S_M \times S_N$ blocks for encryption, where $\sqrt{M} \leq S_M \leq M$ and $\sqrt{N} \leq S_N \leq N$. $\{b(i)\}$ is used to pseudo-randomly control *no*-round $4(S_M + S_N) - 2$ shift operations with four different directions to permute all blocks and all pixels in each block. The CIE (Chaotic Image Encryption) algorithm proposed in [132] is a simplified version of HCIE. Because HCIE is a permutation-only image encryption scheme, it cannot resist the chosen-plaintext attack, and a mask image that is equivalent to the key can still be reconstructed from a small number of pairs of plain-images and cipher-images.

- **MLIE** (*Mirror-Like Image Encryption*) [134] and **CMLIE** (*Chaotic MLIE*) [141,142]: $\{b(i)\}$ is used to pseudo-randomly control four different mirror-like swapping operations within the images. Since the two schemes are both permutation-only image encryption schemes, they cannot resist known/chosen-plaintext attacks.

- **CNNSE** (*Chaotic Neural Network for Signal Encryption*) [135,140,143]: $\{b(i)\}$ is used to control the weights of a neutral network, which is then used to encrypt each pixel bit by bit. The final function of the chaotic neutral network is very simple: $d'_i(n) = d_i(n) \oplus b(8 \times n + i)$, where $d_i(n)$ and $d'_i(n)$ respectively represent the i^{th} plain-bit of the n^{th} plain-pixel and the i^{th} cipher-bit of the n^{th} cipher-pixel. Apparently, this scheme works like a stream cipher, and so CNNSE is vulnerable to known/chosen-plaintext attack: only one known/chosen plaintext is enough to reveal the sequence b and then to derive the secret key. It is the least secure image encryption scheme among all those proposed by Yen et al.

- **TDCEA** (*The 2D Circulation Encryption Algorithm*) [144]: This scheme is an enhanced version of BRIE [136, 137]. For a bit-matrix M composed by 8 consecutive pixel values, $\{b(i)\}$ is used to make bit-shift operations in four different directions. TDCEA has better capability against the known-plaintext attack than BRIE, but it is still not secure enough against the chosen-plaintext attack.

- **DSEA** (*Domino Signal Encryption Algorithm*) [145]: For the n^{th} plain-byte $f(n)$, `true_key` = `initial_key` if $i \bmod L = 0$, else `true_key` $= f'(n-1)$, where $f'(n)$ means the n^{th} cipher-byte. $\{b(n)\}$ is used to pseudo-randomly select an encryption function from XOR and NXOR: if $b(n) = 1$ then $g'(n) = g(n)$ XOR `true_key`, else $g'(n) = g(n)$ NXOR `true_key`. Since a NXOR $b = a$ XOR $\bar{b}$, DSEA cannot resist known/chosen-plaintext attacks.

- **RSES** (*Random Seed Encryption Subsystem*) [147] and **RCES** (*Random Control Encryption Subsystem*) [146]: RESE and RCES are actually the same encryption scheme, which is an enhanced version of CKBA [138]. The two masking keys, $key1, key2$, used in CKBA become time-variant and are pseudo-randomly controlled by $\{b(i)\}$. $\{b(i)\}$ are also used to control swap operations exerted on neighboring pixels. Although this scheme is much more complex than CKBA, it is still insecure against known/chosen-plaintext attacks [151].

Other image encryption schemes based on 1-D chaotic maps

- In [152], another permutation-only image encryption scheme was proposed for binary images. The 1D chaotic map $x(k+1) = \sin(a/x(k))$ is used to pseudo-randomly permutate all pixels. Apparently, it cannot resist known/chosen-plaintext attacks, but it is generally difficult to derive the secret key by breaking the permutation matrix.

- In [103, 104], the Logistic map is used as a chaotic stream cipher (more than a chaotic PRNG) to mask the SPIHT-encoding bit-stream of a wavelet-compressed image. To resist known/chosen-plaintext attacks, three different masking operations are used and the selected operation at each position is dependent on previous cipher-bits.

4.4.4 A Related Topic: Chaos-Based Watermarking

Due to the similarity between image encryption and image watermarking, some ideas of chaos-based image encryption have also been used in the area of digital watermarking [153–157]. Generally speaking, there are two ways to use chaos in a watermarking system: directly generating watermark signals (pattern) from chaos, and mixing (2-D) watermark patterns via chaos. The first way corresponds to chaotic PRNG, and the second to chaotic permutations of 2-D images (i.e. the secret permutation used in image encryption schemes based on 2-D chaotic maps). At present almost all chaos-related techniques used in watermarking systems are borrowed from chaotic cryptography (especially chaos-based image encryption), but it can be expected that some new ideas in chaos-based digital watermarking will also benefit image encryption community in future.

4.4.5 Chaos-Based Video Encryption

SCAN-based encryption for losslessly compressed videos: The new generation of SCAN-based image encryption schemes were also extended to encrypt videos [120, 121, 123, 124]. The plain-video is compressed with a frame-difference-based light lossless compression algorithm, and then encrypted with the new SCAN-based encryption algorithm.

Yen et al.'s encryption schemes for MPEG videos: Some of Yen et al.'s image encryption schemes [134–136, 138, 140–143, 145, 146] were recommended for encrypting MPEG videos, thanks to their high encryption speed. The idea of selective encryption was also used in [136,138]: motion vectors are selected as data for encryption using BRIE or CKBA. However, the insecurity of Yen et al.'s encryption schemes makes their use in video encryption unacceptable.

Chiaraluce et al.'s chaos-based H.263+ encryption scheme: In [158], a chaotic video encryption scheme was proposed for encrypting the following selective data of an H.263+ encoded video: most sign bits of DC coefficients, the AC coefficients of I-macroblocks, sign bits of AC coefficients of P-macroblocks, and sign bits of motion vectors. The proposed scheme is a stream cipher based on three different chaotic maps: the skew tent map, the skew sawtooth map, and the discretized Logistic map. The outputs of the first two chaotic maps are added, and then the addition is scaled to be an integer between 0 and 255. Each scaled integer is used as the initial condition of the third map to generate a 64-size key stream to mask the plaintext with XOR operation. To further enhance the security against known/chosen-plaintext attacks, it was suggested to change the key every 30 frames.

CVES (*Chaotic Video Encryption Scheme*): In [159], a chaos-based encryption scheme called CVES using multiple chaotic systems was proposed. CVES is actually a fast chaotic cipher that encrypts bulky plaintext frame by frame. The basic idea is to combine a simple chaotic stream cipher and a simple chaotic block cipher to construct a fast and secure product cipher. In Chap. 9 of [91], it was pointed out that the original CVES is not sufficiently secure against the chosen-plaintext attack, and an enhanced version of CVES was proposed by adding ciphertext feedback. Figure 4.4 gives a diagrammatic view of the enhanced CVES, where CCS, ECS(1)$\sim$ECS(2^n) are all piecewise linear chaotic maps, and m-LFSR$_1$, m-LFSR$_2$ are the perturbing PRNG of CCS, ECS respectively. The encryption procedure of CVES can be described as follows. Each plain-block is first XORed by a chaotic signal pseudo-randomly selected from chaotic orbits of the 2^n ECS (encryption chaotic systems), and then substituted by a pseudo-random S-box generated from all chaotic orbits of the 2^n ECS. Initial tests have shown that the encryption speed of CVES is competitive with most traditional ciphers, and is only a little slower than the AES reference code.

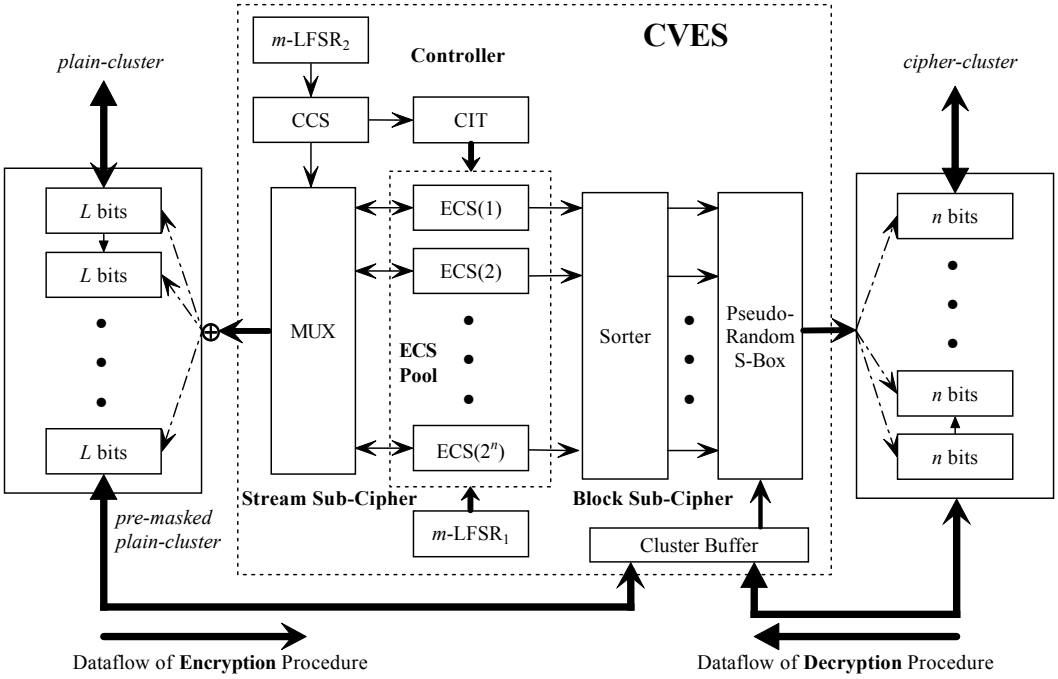


Figure 4.4: The enhanced CVES proposed in Chap. 9 of [91]

4.5 Experiences and Lessons

From the above survey on chaos-based image/video encryption schemes, one can learn some experiences and also lessons on how to design a fast and secure image/video encryption scheme with or without using chaos. Although some experiences and lessons are merely common rules in modern cryptography, for some reasons they have not been widely accepted by the image/video encryption community. In this section, we summarize these learned experiences and lessons, in the following list of remarks.

Remark 1 *Permutation-only image/video encryption schemes are generally insecure against known/chosen-plaintext attacks.*

Under known/chosen-plaintext attacks, a mask image that is equivalent to the secret key can be obtained to decrypt cipher-images encrypted with the same key. In addition, permutation-only image ciphers cannot change plain-histograms, which contain some useful information about the plain-images: for example, cartoon pictures and real photos have different histograms, and photos of human faces usually have narrower histograms than photos of natural scenes.

Remark 2 *Secret permutation is NOT a prerequisite of a secure image/video encryption scheme.*

This is because the substitution part running in CBC mode is sufficient for achieving confusion and diffusion properties, and for ensuring security against the chosen-ciphertext attack. In fact, comparing Fig. 8 and Fig. 13 of [98], one can see that the substitution algorithm can make the cipher-image look "chaotic" much faster than a chaotic permutation. This implies the incapability of chaotic permutations. It is believed that the main reason to use secret chaotic permutation in an image/video encryption scheme is that secret permutation MAY be useful to increase the computational complexity of a potential chosen-plaintext attack. With the use of secret permutation, the statistical cryptanalysis of the concerned encryption scheme will become much more complicated or impractical.

Remark 3 *Ciphertext feedback is very useful for enhancing the security against known/chosen-plaintext attacks.*

Most image encryption schemes based on 2-D chaotic maps, the new generation of SCAN-based image encryption schemes, and the enhanced CVES all utilize the ciphertext feedback mechanism to resist the chosen-plaintext attack.

Remark 4 *Combining the ciphertext feedback and a (secret) permutation can achieve the diffusion (i.e., avalanche) property at the level of image/video-frame.*

Although secret permutations are commonly used together with the ciphertext feedback to provide the diffusion property, the permutation can actually be publicized. Apparently, using a public permutation only means that the secret key of the secret permutation is publicized so that the security relies on other parts of the whole cryptosystem.

Remark 5 *Combining a simple stream cipher and a simple block cipher running in CBC mode can yield a secure and fast encryption scheme, where the stream cipher is used to create the confusion property, the block cipher is used to realize the diffusion property, and the ciphertext feedback in CBC mode is used to resist the chosen-plaintext attack.*

The modified CVES proposed in Chap. 9 of [91] is a one-round version of such a simple but fast encryption scheme. In CVES, the avalanche property is sacrificed in order to increase the encryption speed. The loss of the avalanche feature may not influence the security of the schemes, however.

Remark 6 *The diffusion methods used in most chaos-based encryption schemes are too slow due to the multiple time-consuming iteration of chaotic permutations.*

In fact, only two rounds are enough to achieve diffusion: encrypt the data in CBC mode from top to bottom, and then encrypt the partially-encrypted data again in CBC mode from bottom to top.

Remark 7 *Selective encryption may provide enough security, if the unencrypted data are dependent on the encrypt data.*

An example of such selective encryption schemes is the one proposed in [53], which is based on the context-sensitive compression algorithm. More studies are needed to clarify the relationship between the selective encryption and the model-based compression algorithms.

Remark 8 *Although the selective encryption is generally insecure from the cryptographical point of view, it can be generalized to provide a more general way for designing fast and secure video encryption schemes: use a slow (but stronger) cipher to encrypt selective data, and use a fast (but weaker) cipher to encrypt the rest data.*

Two video ciphers were constructed in [90] to show the potential of this idea. In the case that the compression algorithm is antagonistic to the simple selective encryption, this generalized version of selective encryption will be very useful as a replacement for the simple one.

4.6 Conclusions

Image and video encryption plays a more and more important role in today's multimedia world. Although many encryption schemes have been proposed to provide security for digital images and videos, some of them are too weak to resist various attacks designed by cryptanalysts. Basically, many efforts have been devoted to study the security issue, but for multimedia the security is still not strong from a serious cryptographic point of view. To design a truly secure image/video encryption scheme, the classical cryptology must be employed.

As an emerging tool for the design of digital ciphers, chaos theory has been widely investigated especially to develop image and video encryption algorithms. The simplicity of many discrete chaotic maps and the well-established chaos theory make it possible to approach practically good solutions to image and video encryption. The success and failur of chaos-based encryption schemes have led to some valuable experiences and lessons, which can be used as the fundamentals of future research on the chaos-based multimedia encryption technology. At this point, chaos theory for image/video encryption appears to be promising but not yet mature. More efforts are needed for its further development toward a marketable future.

Acknowledgements

The authors would like to thank Dr. Gonzalo Álvarez at Instituto de Física Aplicada of Consejo Superior de Investigaciones Científicas (Spain), Dr. Ennio Gambi at Universitá di Ancona (Italy), and Mr. Chengqing Li at Zhejiang University (China), for their valuable comments on the manuscript of this chapter.

Bibliography

[1] Bruce Schneier. *Applied Cryptography – Protocols, Algorithms, and Souce Code in C.* John Wiley & Sons, Inc., New York, second edition, 1996.

[2] Philip P. Dang and Paul M. Chau. Image encryption for secure internet multimedia applications. *IEEE Trans. Consumer Eletronics*, 46(3):395–403, 2000.

[3] Philip P. Dang and Paul M. Chau. Implementation IDEA algorithm for image encryption. In *Mathematics and Applications of Data/Image Coding, Compression, and Encryption III*, volume 4122 of *Proceedings of SPIE*, pages 1–9, 2000.

[4] Philip P. Dang and Paul M. Chau. Hardware/software implementation 3-Way algorithm for image encryption. In *Security and Watermarking of Multimedia Contents II*, volume 3971 of *Proceedings of SPIE*, pages 274–283, 2000.

[5] Steven McCanne and Van Jacobson. vic: A flexible framework for packet video. In *Proc. 3rd ACM Int. Conference on Multimedia*, pages 511–522, 1995.

[6] Lintian Qiao. *Multimedia Security and Copyright Protection.* PhD thesis, Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, Illinois, USA, 1998.

[7] Lintian Qiao and Klara Nahrsted. Comparison of MPEG encryption algorithms. *Computers & Graphics*, 22(4):437–448, 1998.

[8] Iskender Agi and Li Gong. An empirical study of secure MPEG video transmission. In *Proc. ISOC Symposium on Network and Distributed Systems Security (SNDSS'96)*, pages 137–144, 1996.

[9] Tom D. Lookabaugh, Douglas C. Sicker, David M. Keaton, Wang Y. Guo, and Indrani Vedula. Security analysis of selectively encrypted MPEG-2 streams. In *Multimedia Systems and Applications VI*, volume 5241 of *Proceedings of SPIE*, pages 10–21, 2003.

[10] Chung-Ping Wu and C.-C. Jay Kuo. Fast encryption methods for audiovisual data confidentiality. In *Multimedia Systems and Applications III*, volume 4209 of *Proceedings of SPIE*, pages 284–295, 2001.

[11] Andreas Pommer and Andreas Uhl. Application scenarios for selective encryption of visual data. In *Proc. Multimedia and Security Workshop of 10th ACM Int. Conference on Multimedia*, pages 71–74, 2002.

[12] Ibrahim E. Ziedan, Mohammed M. Fouad, and Doaa H. Salem. Application of data encryption standard to bitmap and JPEG images. In *Proc. 12th National Radio Science Conference (NRSC'2003)*, pages C16/1–C16/8, 2003.

[13] Jiangtao Wen, Michael Severa, Wenjun Zeng, Maximilian H. Luttrell, and Weiyi Jin. A format-compliant configurable encryption framework for access control of video. *IEEE Trans. Circuits and Systems for Video Technology*, 12(6):545–557, 2002.

[14] Benoît M. Macq and Jean-Jacques Quisquater. Cryptology for digital TV broadcasting. *Proceedings of the IEEE*, 83(6):944–957, 1995.

[15] Jiangtao Wen, Mike Severa, Wenjun Zeng, Maximilian H. Luttrell, and Weiyi Jin. A format-compliant configurable encryption framework for access control of multimedia. In *Proc. IEEE 4th Workshop on Multimedia Signal Processing (MMSP'2001)*, pages 435–440, 2001.

[16] Susie J. Wee and John Apostolopoulos. Secure scablable streaming and secure transcoding with JPEG2000. In *Proc. IEEE Int. Conference on Image Processing (ICIP'2003)*, volume I, pages 205–208, 2003.

[17] Hong Heather Yu and Xiaolong Yu. Progressive and scalable encryption for multimedia content access control. In *Proc. IEEE Int. Conference on Communications (ICC'2003)*, volume 1, pages 547–551, 2003.

[18] Chun Yuan, Bin B. Zhu, Yidong Wang, Shipeng Li, and Yuzhuo Zhong. Efficient and fully scalable encryption for MPEG-4 FGS. In *Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2003)*, volume II, pages 620–623, 2003.

[19] Ahmet M. Eskicioglu and Edward J. Delp. An integrated approach to encrypting scabable video. In *Proc. IEEE Int. Conference on Multimedia and Expo (ICME'2002)*, pages 573–576, 2002.

[20] Susie J. Wee and John G. Apostolopoulos. Secure scablable streaming enabling transcoding without decryption. In *Proc. IEEE Int. Conference on Image Processing (ICIP'2001)*, volume 1, pages 437–440, 2001.

[21] Susie J. Wee and John G. Apostolopoulos. Secure scablable video streaming for wireless networks. In *Proc. IEEE Int. Conference on Acoustics, Speech, and Signal Processing (ICASSP'2001)*, volume 4, pages 2049–2052, 2001.

[22] Ali Şaman Tosun and Wu-chi Feng. Lightweight security mechanisms for wireless video transmission. In *Proc. IEEE Int. Conference on Information Technology: Coding and Computing*, pages 157–161, 2001.

[23] Ali Şaman Tosun and Wu-chi Feng. Efficient multi-layer coding and encryption of MPEG video streams. In *Proc. IEEE Int. Conference on Multimedia and Expo (ICME'2000)*, pages 119–122, 2000.

[24] Thomas Kunkelmann and Uwe Horn. Partial video encryption based on scalable coding. In *Proc. 5th Int. Workshop on Systems, Signals and Image Processing (IWSSIP'98)*, 1998.

[25] Jana Dittmann and Arnd Steinmetz. Enabling technology for the trading of MPEG-encoded video. In *Information Security and Privacy: Second Australasian Conference (ACISP'97) Proc.*, volume 1270 of *Lecture Notes in Computer Science*, pages 314–324, 1997.

[26] David S. Taubman and Michael W. Marcellin. JPEG2000: Standard for interactive imaging. *Proceedings of the IEEE*, 90(8):1336–1357, 2002.

[27] Weiping Li. Overview of fine granularity scalability in MPEG-4 video standard. *IEEE Trans. Circuits and Systems for Video Technology*, 11(3):301–317, 2001.

[28] Andrés Torrubia and Francisco Mora. Perceptual cryptography of JPEG compressed images on the JFIF bitstream domain. In *Digest of Technical Papers of IEEE Int. Conference on Consumer Electronics (ICCE'2003)*, pages 58–59, 2003.

[29] Andrés Torrubia and Francisco Mora. Perceptual cryptography on MPEG layer III bit-streams. *IEEE Trans. Consumer Eletronics*, 48(4):1046–1050, 2002.

[30] Stéphane Roche, Jean-Luc Dugelay, and Refik Molva. Multi-resolution access control algorithm based on fractal coding. In *Proc. IEEE Int. Conference on Image Processing (ICIP'96)*, volume 3, pages 235–238, 1996.

[31] Said E. El-Khamy and Hossam El-Din M. Abdou. A novel secure image coding scheme using fractal transformation. In *Proc. 15th (Egypt) National Radio Science Conference (NRSC'98)*, pages C23/1–C23/9, 1998.

[32] Raphaël Grosbois, Pierre Gerbelot, and Touradj Ebrahimi. Authentication and access control in the JPEG 2000 compressed domain. In *Applications of Digital Image Processing XXIV*, volume 4472 of *Proceedings of SPIE*, pages 95–104, 2001.

[33] Marc Van Droogenbroeck and Raphaël Benedett. Techniques for a selective encryption of uncompressed and compressed images. In *Proc. Advanced Concepts for Intelligent Vision Systems (ACIVS'2002)*, pages 90–97, 2002.

[34] Dimitrious Simitopoulos, Nikolaos Zissis, Panagiotis Georgiadis, Vasileios Emmanouilidis, and Michael G. Strintzis. Encryption and watermarking for the secure distribution of copyrighted MPEG video on DVD. *Multimedia Systems*, 9(3):217–227, 2003.

[35] Hitoshi Kiya, Dhoko Imaizumi, and Osamu Watanabe. Partial-scrambling of images encoded using JPEG2000 without generating marker codes. In *Proc. IEEE Int. Conference on Image Processing (ICIP'2003)*, volume III, pages 205–208, 2003.

[36] Yann Bodo, Nathalie Laurent, and Jean-Luc Dugelay. A scrambling method based on disturbance of motion vector. In *Proc. 10th ACM Int. Conference on Multimedia*, pages 89–90, 2002.

[37] Melih Pazarci and Vadi Dipçin. A MPEG2-transparent scrambling technique. *IEEE Trans. Consumer Eletronics*, 48(2):345–355, 2002.

[38] Ali Şaman Tosun and Wu-chi Feng. On error preserving encryption algorithms for wireless video transmission. In *Proc. 9th ACM Int. Conference on Multimedia*, pages 302–308, 2001.

[39] Takeyuki Uehara, Reihaneh Safavi-Naini, and Philip Ogunbona. Securing wavelet compression with random permutations. In *Proc. IEEE Pacific-Rim Conference on Multimedia (IEEE-PCM'2000)*, pages 332–335, 2000.

[40] Andreas Pommer and Andreas Uhl. Wavelet packet methods for multimedia compression and encryption. In *Proc. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM'2001)*, volume 1, pages 1–4, 2001.

[41] Andreas Pommer. *Selective Encryption of Wavelet-Compressed Visual Data*. PhD thesis, Department of Scientific Computing, University of Salzburg, Austria, June 2003.

[42] Andreas Pommer and Andreas Uhl. Selective encryption of wavelet-packet encoded image data: Efficiency and security. *Multimedia Systems*, 9(3):279–287, 2003.

[43] Young-Ho Seo, Dong-Wook Kim, Ji-Sang Yoo, Sujit Dey, and Abhishek Agrawal. Wavelet domain image encryption by subband selection and data bit selection. In *Proc. World Wireless Congress (WCC'03/3GWireless'2003)*, 2003.

[44] ISO. MPEG4 IPMP (Intellectual Property Management and Protection) Final Proposed Draft Amendment (FPDAM). ISO/IEC 14496-1:2001/AMD3, ISO/IEC JTC 1/SC 29/WG11 N4701, March 2002.

[45] Thomas Kunkelmann, Rolf Reinema, Ralf Steinmetz, and Thomas Blecher. Evaluation of different video encryption methods for a secure multimedia conferencing gateway. In *From Multimedia Services to Network Services: 4th Int. COST 237 Workshop Proc.*, volume 1356 of *Lecture Notes in Computer Science*, pages 75–89, 1997.

[46] Thomas Kunkelmann and Uwe Horn. Video encryption based on data partitioning and scalable coding - a comparison. In *Interactive Distributed Multimedia Systems and Telecommunication Services: 5th Int. Workshop (IDMS'98) Proc.*, volume 1483 of *Lecture Notes in Computer Science*, pages 95–106, 1998.

[47] Xiliang Liu and Ahmet M. Eskicioglu. Selective encryption of multimedia content in distribution networks: Challenges and new directions. In *Proc. IASTED Int. Conference on Communications, Internet and Information Technology (CIIT'2003)*, 2003.

[48] George Anatassios Spanos and Tracy Bradley Maples. Security for real-time MPEG compressed video in distributed multimedia applications. In *Proc. IEEE 15th Annual Int. Phoenix Conference on Computers and Communications*, pages 72–78, 1996.

[49] Justin H. Dolske. Secure MPEG video: Techniques and pitfalls. available online at `http://www.dolske.net/old/gradwork/cis788r08/`, June 1997.

[50] Champskud J. Skrepth and Andreas Uhl. Selective encryption of visual data. In *Proc. IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security (CMS'2002)*, pages 213–226, 2002.

[51] Howard Chi Ho Cheng. Partial encryption for image and video communication. Master's thesis, Department of Computing Science, University of Alberta, Edmonton, Alberta, Canada, Fall 1998.

[52] Lintian Qiao and Klara Nahrstedt. A new algorithm for MPEG video encryption. In *Proc. 1st Int. Conference on Imaging Science, Systems, and Technology (CISST'97)*, pages 21–29, 1997.

[53] Xiaolin Wu and Peter W. Moo. Joint image/video compression and encryption via high-order conditional entropy coding of wavelet coefficients. In *Proc. IEEE Conference on Multimedia Computing and Systems (CMS'99)*, pages 908–912, 1999.

[54] Lei Tang. Methods for encrypting and decrypting MPEG video data efficiently. In *Proc. 4th ACM Int. Conference on Multimedia*, pages 219–229, 1996.

[55] Chandrapal Kailasanathan, Reihaneh Safavi-Naini, and Philip Ogunbona. Compression performance of JPEG encryption scheme. In *Proc. 14th Int. Conference on Digital Signal Processing (DSP'2002)*, volume 2, pages 1329–1332, 2002.

[56] Changgui Shi and Bharat Bhargava. Light-weight MPEG video encryption algorithm. In *Proc. Int. Conference on Multimedia (Multimedia'98, Shaping the Future*, pages 55–61, 1998.

[57] Bharat Bhargava, Changgui Shi, and Sheng-Yih Wang. MPEG video encryption algorithms. *Multimedia Tools and Applications*, 24(1):57–79, 2004.

[58] Chung-Ping Wu and C.-C. Jay Kuo. Efficient multimedia encryption via entropy codec design. In *Security and Watermarking of Multimedia Contents III*, volume 4314 of *Proceedings of SPIE*, pages 128–138, 2001.

[59] Dahua Xie and C.-C. Jay Kuo. An enhanced MHT encryption scheme for chosen plaintext attack. In *Internet Multimedia Management Systems IV*, volume 5242 of *Proceedings of SPIE*, pages 175–183, 2003.

[60] Mohan S. Kankanhalli and Teo Tian Guan. Compressed-domain scrambler/descrambler for digital video. *IEEE Trans. Consumer Eletronics*, 48(2):356–365, 2002.

[61] Wenjun Zeng and Shawmin Lei. Efficient frequency domain video scrambling for content access control. In *Proc. 7th ACM Int. Conference on Multimedia*, pages 285–294, 1999.

[62] Wenjun Zeng and Shawmin Lei. Efficient frequency domain selective scrambling of digital video. *IEEE Trans. Multimedia*, 5(1):118–129, 2003.

[63] Xiaobo Li, Jason Knipe, and Howard Cheng. Image compression and encryption using tree structures. *Pattern Recognition Letters*, 18(8):2439–2451, 1997.

[64] Howard Cheng and Xiaobo Li. Partial encryption of compressed images and videos. *IEEE Trans. Signal Processing*, 48(8):2439–2451, 2000.

[65] Howard Cheng and Xiaobo Li. On the application of image decomposition to image compression and encryption. In *Communications and Multimedia Security II: Proc. IFIP TC6/TC11 Int. Conference (CMS'96)*, pages 116–127, 1996.

[66] Martina Podesser, Hans-Peter Schmidt, and Andreas Uhl. Selective bitplane encryption for secure transmission of image data in mobile environments. In *Proc. 5th IEEE Nordic Signal Processing Symposium (NORSIG'2002)*, 2002.

[67] Roland Norcen, Martina Podesser, Andreas Pommer, Hans-Peter Schmidt, and Andreas Uhl. Confidential storage and transmission of medical image data. *Computers in Biology and Medicine*, 33(3):277–292, 2003.

[68] Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen. A new encryption algorithm for image cryptosystems. *J. Systems and Software*, 58(2):83–91, 2001.

[69] Shiguo Lian and Zhiquan Wang. Comparison of several wavelet coefficients confusion methods applied in multimedia encryption. In *Proc. Int. Conference on Computer Networks and Mobile Computing (ICCNMC'2003)*, pages 372–376, 2003.

[70] Roland Norcen and Andreas Uhl. Selective encryption of the JPEG2000 bitstream. In *Proc. IFIP TC6/TC11 7th Joint Working Conference on Communications and Multimedia Security (CMS'2003)*, volume 2828 of *Lecture Notes in Computer Science*, pages 194–204, 2003.

[71] Lutz Vorwerk, Thomas Engel, and Christoph Meinel. A proposal for a combination of compression and encryption. In *Visual Communications and Image Processing 2000*, volume 4067 of *Proceedings of SPIE*, pages 694–702, 2000.

[72] Andreas Pommer and Andreas Uhl. Multimedia soft encryption using NSMRA wavelet packet methods: Parallel attacks. In *Proc. Int. Workshop on Parallel Numerics (ParNum'2000)*, pages 179–190, 2000.

[73] Roland Norcen and Andreas Uhl. Selective encryption of wavelet packet subband structures for obscured transmission of visual data. In *Proc. 3rd IEEE Benelux Signal Processing Symposium (SPS'2002)*, pages 25–28, 2002.

[74] Roland Norcen and Andreas Uhl. Selective encryption of wavelet packet subband structures for secure transmission of visual data. In *Proc. Multimedia and Security Workshop of 10th ACM Int. Conference on Multimedia*, pages 67–70, 2002.

[75] Trees-Juen Chuang and Ja-Chen Lin. New approach to image encryption. *J. Electronic Imaging*, 7(2):350–356, 1998.

[76] Jürgen Meyer and Frank Gadegast. *Security Mechanisms for Multimedia-Data with the Example MPEG-1 Video*. Berlin, Germany, 1995. The description of the project SECMPEG, available online at `http://www.gadegast.de/frank/doc/secmeng.pdf`.

[77] Nut Taesombut, Richard Huang, and Venkat P. Rangan. A secure multimedia system in emerging wireless home networks. In *Communications and Multimedia Security (CMS'2003)*, volume 2828 of *Lecture Notes in Computer Science*, pages 76–88, 2003.

[78] Thomas Kunkelmann and Rolf Reinema. A scalable security architecture for multimedia communication standards. In *Proc. IEEE Int. Conference on Multimedia Computing and Systems (ICMCS'97)*, pages 660–661, 1997.

[79] Yongcheng Li, Zhigang Chen, See-Mong Tan, and Roy H. Campbell. Security enhanced MPEG player. In *Proc. Int. Workshop on Multimedia Software Development (MMSD'96)*, pages 169–175, 1996.

[80] George Anatassios Spanos and Tracy Bradley Maples. Performance study of a selective encryption scheme for the security of networked, real-time video. In *Proc. 4th Int. Conference on Computer Communications and Networks (IC3N'95)*, pages 2–10, 1995.

[81] Adnan M. Alattar and Ghassan I. Al-Regib. Evaluation of selective encryption techniques for secure transmission of MPEG video bit-streams. In *Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'99)*, volume IV, pages 340–343, 1999.

[82] Sang Uk Shin, Kyeong Seop Sim, and Kyung Hyune Rhee. A secrecy scheme for MPEG video data using the joint of compression and encryption. In *Information Security: Second Int. Workshop (ISW'99) Proc.*, volume 1729 of *Lecture Notes in Computer Science*, pages 191–201, 1999.

[83] Wenjun Zeng, Jiangtao Wen, and Mike Severa. Fast self-synchronous content scrambling by spatially shuffling codewords of compressed bitstream. In *Proc. IEEE Int. Conference on Image Processing (ICIP'2002)*, volume III, pages 169–172, 2002.

[84] Lintian Qiao, Klara Nahrstedt, and Ming-Chit Tam. Is MPEG encryption by using random list instead of ZigZag order secure? In *Proc. IEEE Int. Symposium on Consumer Electronics (ISCE'97)*, pages 226–229, 1997.

[85] Takeyuki Uehara and Reihaneh Safavi-Naini. Chosen DCT coefficients attack on MPEG encryption schemes. In *Proc. IEEE Pacific-Rim Conference on Multimedia (IEEE-PCM'2000)*, pages 316–319, 2000.

[86] Changgui Shi and Bharat Bhargava. An efficient MPEG video encryption algorithm. In *Proc. IEEE Symposium on Reliable Distrubited Systems*, pages 381–386, 1998.

[87] Changgui Shi and Bharat Bhargava. A fast MPEG video encryption algorithm. In *Proc. 6th ACM Int. Conference on Multimedia*, pages 81–88, 1998.

[88] Changgui Shi, Sheng-Yih Wang, and Bharat Bhargava. MPEG video encryption in real-time using secret key cryptography. In *Proc. Int. Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'99)*, pages 191–201, 1999.

[89] Melih Pazarci and Vadi Dipçin. A MPEG-transparent scrambling technique. *IEEE Trans. Consumer Eletronics*, 48(2):345–355, 2002.

[90] Feng Bao, Robert Deng, Peirong Feng, Yan Guo, and Hongjun Wu. Secure and private distribution of online video and some related cryptographic issues. In *Information Security and Privacy: The 6th Australasian Conference (ACISP 2001) Proc.*, volume 2119 of *Lecture Notes in Computer Science*, pages 190–205, 2001.

[91] Shujun Li. *Analyses and New Designs of Digital Chaotic Ciphers*. PhD thesis, School of Electronics & Information Engineering, Xi'an Jiaotong University, Xi'an, China, June 2003. Available online at `http://www.hooklee.com/pub.html` (in both Chinese and English).

[92] Franz Pichler and Josef Scharinger. Finite dimensional generalized Baker dynamical systems for cryptographic applications. In *Prof. 5th Int. Workshop on Computer Aidded Systems Theory (EuroCAST'95)*, volume 1030 of *Lecture Notes in Computer Science*, pages 465–476, 1996.

[93] Josef Scharinger. Fast encryption of image data using chaotic Kolmogorov flows. In *Storage and Retrieval for Image and Video Databases V*, volume 3022 of *Proceedings of SPIE*, pages 278–289, 1997.

[94] Josef Scharinger. Secure and fast encryption using chaotic Kolmogorov flows. In *Proc. IEEE Information Theory Workshop (ITW'98)*, pages 124–125, 1998.

[95] Josef Scharinger. Fast encryption of image data using chaotic Kolmogorov flows. *J. Electronic Imaging*, 7(2):318–325, 1998.

[96] Jiri Fridrich. Image encryption based on chaotic maps. In *Proc. IEEE Int. Conference on Sysytems, Man and Cybernetics (ICSMC'97)*, volume 2, pages 1105–1110, 1997.

[97] Jiri Fridrich. Secure image ciphering based on chaos. Technical Report RL-TR-97-155, the Information Directorate (former Rome Laboratory) of the Air Force Research Laboratory, New York, USA, March 1997.

[98] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcation and Chaos*, 8(6):1259–1284, 1998.

[99] Mazleena Salleh, Subariah Ibrahim, and Ismail Fauzi Isinn. Ciphering key of chaos image encryption. In *Proc. Int. Conference on Artificial Intelligence in Engineering and Technology (ICAIET'2002)*, pages 58–62, 2002.

[100] Mazleena Salleh, Subariah Ibrahim, and Ismail Fauzi Isinn. Enhanced chaotic image encryption algorithm based on Baker's map. In *Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2003)*, volume II, pages 508–511, 2003.

[101] Dongxu Qi, Jiancheng Zou, and Xiaoyou Han. A new class of scrambling transformation and its application in the image information covering. *Science in China - Series E (English Ed.)*, 43(3):304–312, 2000.

[102] Yaobin Mao, Guanrong Chen, and Shiguo Lian. A novel fast image encryption scheme based on 3D chaotic Baker maps. *Int. J. Bifurcation and Chaos*, 14(10):3613–3624, 2004.

[103] Yaobin Mao and Guanrong Chen. Chaos-based image encryption. In Eduardo Bayro-Corrochano, editor, *Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neural Computing and Robotics*. Springer-Verlag, Heidelberg, April 2004.

[104] Yaobin Mao. *Research on Chaos-based Image Encryption and Watermarking Technology*. PhD thesis, Department of Automatation, Nanjing University of Science & Technology, Nanjing, China, August 2003. (in Chinese).

[105] Yaobin Mao, Guanrong Chen, and Charles K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3):749–761, 2004.

[106] Masaki Miyamoto, Kiyoshi Tanaka, and Tatsuo Sugimura. Truncated Baker transformation and its extension to image encryption. In *Mathematics of Data/Image Coding, Compression, and Encryption II*, volume 3814 of *Proceedings of SPIE*, pages 13–25, 1999.

[107] Kenji Yano and Kiyoshi Tanaka. Image encryption scheme based on a truncated Baker transformation. *IEICE Trans. Fundamentals*, E85-A(9):2025–2035, 2002.

[108] Rodolfo Zunino. Fractal circuit layout for spatial decorrelation of images. *Electronics Letters*, 34(20):1929–1930, 1998.

[109] S. Bottini. An algebraic model of an associative noise-like coding memory. *Biological Cybernetics*, 36(4):221–228, 1980.

[110] Giancarlo Parodi, Sandro Ridella, and Rodolfo Zunino. Using chaos to generate keys for associative noise-like coding memories. *Neural Networks*, 6(4):559–572, 1993.

[111] Yossi Matias and Adi Shamir. A video scrambing technique based on space filling curve (extended abstract). In *Advances in Cryptology – Crypto'87*, volume 293 of *Lecture Notes in Computer Science*, pages 398–417, 1987.

[112] Michael Bertilsson, Ernest F. Brickell, and Ingemar Ingemarson. Cryptanalysis of video encryption based on space-filling curves. In *Advances in Cryptology – EuroCrypt'88*, volume 434 of *Lecture Notes in Computer Science*, pages 403–411, 1989.

[113] Nikolaos G. Bourbakis and Chris Alexopoulos. A fractal-based image processing language: Formal modeling. *Pattern Recognition*, 32(2):317–338, 1999.

[114] Nikolaos G. Bourbakis and Chris Alexopoulos. Picture data encryption using SCAN patterns. *Pattern Recognition*, 25(6):567–581, 1992.

[115] Chris Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou. Image encryption method using a class of fractals. *J. Electronic Imaging*, 4(3):251–259, 1995.

[116] Nikolaos G. Bourbakis. Image data compression-encryption using G-SCAN pattern. In *Proc. IEEE Int. Conference on Systems, Man and Cybernetics*, volume 2, pages 1117–1120, 1997.

[117] Henry Key-Chang Chang and Jiang-Long Liu. A linear quadtree compression scheme for image encryption. *Signal Processing: Image Communication*, 10(4):279–290, 1997.

[118] Kuo-Liang Chung and Lung-Chun Chang. Large encryption binary images with higher security. *Pattern Recognition Letters*, 19(5–6):461–468, 1998.

[119] Suchindran S. Maniccam and Nikolaos G. Bourbakis. SCAN based lossless image compression and encryption. In *Proc. IEEE Int. Conference on Information Intelligence and Systems (ICIIS'99)*, pages 490–499, 1999.

[120] Nikolaos G. Bourbakis and Apostolos Dollas. SCAN-based compression-encryption-hiding for video on demand. *IEEE Multimedia*, 10(3):79–87, 2003.

[121] Suchindran S. Maniccam and Nikolaos G. Bourbakis. Image and video encryption using SCAN patterns. *Pattern Recognition*, 37(4):725–737, 2004.

[122] Nikolaos G. Bourbakis, Rüdiger Brause, and Chris Alexopoulos. SCAN image compression/encryption hardware system. In *Digital Video Compression: Algorithms and Technologies 1995*, volume 2419 of *Proceedings of SPIE*, pages 419–428, 1995.

[123] Apostolos Dollas, Christopher Kachris, and Nikolaos G. Bourbakis. Performance analysis of fixed, reconfigurable, and custom architectures for the SCAN image and video encryption algorithm. In *Proc. 11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'2003)*, pages 19–28, 2003.

[124] Christopher Kachris, Nikolaos G. Bourbakis, and Apostolos Dollas. A reconfigurable logic-based processor for the SCAN image and video encryption algorithm. *Int. J. Parallel Programming*, 31(6):489–506, 2003.

[125] Jinn-Ke Jan and Yuh-Min Tseng. On the security of image encryption method. *Information Processing Letters*, 60(5):261–265, 1996.

[126] Chin-Chen Chang and Tai-Xing Yu. Cryptanalysis of an encryption scheme for binary images. *Pattern Recognition Letters*, 23(14):1847–1852, 2002.

[127] Krish M. Roskin and Jonathan B. Casper. From chaos to cryptography. Available online at `http://xcrypt.theory.org/paper`, 1999.

[128] K. Murali, Haiyang Yu, Vinay Varadan, and Henry Leung. Secure communication using a chaos based signal encryption scheme. *IEEE Trans. Consumer Eletronics*, 47(4):709–714, 2001.

[129] Jun Peng, Xiaofeng Liao, and Zhongfu Wu. Digital image secure communication using Chebyshev map sequences. In *Proc. IEEE Int. Conference on Communications, Circuits and Systems and West Sino Expositions (ICCCS'2002)*, pages 492–496, 2002.

[130] K. Murali, Henry Leung, K. Shakthi Preethi, and I. Raja Mohamed. Spread spectrum image encoding and decoding using ergodic chaos. *IEEE Trans. Consumer Eletronics*, 49(1):59–63, 2003.

[131] Jui-Cheng Yen and Jiun-In Guo. A new hierarchical chaotic image encryption algorithm and its hardware architecture. In *Proc. 9th (Taiwan) VLSI Design/CAD Symposium*, 1998.

[132] Jui-Cheng Yen and Jiun-In Guo. A new chaotic image encryption algorithm. In *Proc. (Taiwan) National Symposium on Telecommunications*, pages 358–362, 1998.

[133] Jiun-In Guo, Jui-Cheng Yen, and Jen-Chieh Yeh. The design and realization of a new hierarchical chaotic image encryption algorithm. In *Proc. Int. Symposium on Communications (ISCOM'99)*, pages 210–214, 1999.

[134] Jiun-In Guo and Jui-Cheng Yen. A new mirror-like image encryption algorithm and its VLSI architecture. In *Proc. 10th (Taiwan) VLSI Design/CAD Symposium*, pages 327–330, 1999.

[135] Jui-Cheng Yen and Jiun-In Guo. A chaotic neural network for signal encryption/decryption and its VLSI architecture. In *Proc. 10th (Taiwan) VLSI Design/CAD Symposium*, pages 319–322, 1999.

[136] Jui-Cheng Yen and Jiun-In Guo. A new MPEG/encryption system and its VLSI architecture. In *Proc. Int. Symposium on Communications (ISCOM'99)*, pages 215–219, 1999.

[137] Jui-Cheng Yen and Jiun-In Guo. A new image encryption algorithm and its VLSI architecture. In *Proc. IEEE Workshop on Signal Processing Systems (SiPS'99)*, pages 430–437, 1999.

[138] Jui-Cheng Yen and Jiun-In Guo. A new chaotic key-based design for image encryption and decryption. In *Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2000)*, volume 4, pages 49–52, 2000.

[139] Jui-Cheng Yen and Jiun-In Guo. Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation. *IEE Proc.–Vision, Image and Signal Processing*, 147(2):167–175, 2000.

[140] Scott Su, Alvin Lin, and Jui-Cheng Yen. Design and realization of a new chaotic neural encryption/decryption network. In *Proc. IEEE Asia-Pacific Conference on Circuits and Systems (APCCAS'2000)*, pages 335–338, 2000.

[141] Jui-Cheng Yen and Jiun-In Guo. A new chaotic mirror-like image encryption algorithm and its VLSI architechture. *Pattern Recognition and Image Analysis (Advances in Mathematical Theory and Applications)*, 10(2):236–247, 2000.

[142] Jiun-In Guo, Jui-Cheng Yen, and Jo-Yo Lin. The FPGA realization of a new image encryption/decryption design. In *Proc. 12th (Taiwan) VLSI Design/CAD Symposium*, 2001.

[143] Jui-Cheng Yen and Jiun-In Guo. The design and realization of a chaotic neural signal security system. *Pattern Recognition and Image Analysis (Advances in Mathematical Theory and Applications)*, 12(1):70–79, 2002.

[144] Jui-Cheng Yen and Jiun-In Guo. Design of a new signal security system. In *Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2002)*, volume IV, pages 121–124, 2002.

[145] Jui-Cheng Yen and Jiun-In Guo. The design and realization of a new domino signal security system. *Journal of the Chinese Institute of Electrical Engineering (Transactions of the Chinese Institute of Engineers, Series E)*, 10(1):69–76, 2003.

[146] Hun-Chen Chen and Jui-Cheng Yen. A new cryptography system and its VLSI realization. *J. Systems Architechture*, 49(7–9):355–367, 2003.

[147] Hun-Chen Chen, Jiu-Cheng Yen, and Jiun-In Guo. Design of a new cryptography system. In *Advances in Multimedia Information Processing - PCM 2002: Third IEEE Pacific Rim Conference on Multimedia Proc.*, volume 2532 of *Lecture Notes in Computer Science*, pages 1041–1048, 2002.

[148] Andrzej Lasota and Michael C. Mackey. *Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics.* Springer-Verlag, New York, second edition, 1997.

[149] Shujun Li and Xuan Zheng. On the security of an image encryption method. In *Proc. IEEE Int. Conference on Image Processing (ICIP'2002)*, volume 2, pages 925–928, 2002.

[150] Shujun Li and Xuan Zheng. Cryptanalysis of a chaotic image encryption method. In *Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2002)*, volume II, pages 708–711, 2002.

[151] Shujun Li, Chengqing Li, Guanrong Chen, and Xuanqin Mou. Cryptanalysis of the RCES/RSES image encryption scheme. submitted to IEEE Trans. Image Processing in 2004.

[152] Fethi Belkhouche and Uvais Qidwai. Binary image encoding using 1D chaotic maps. In *Proc. Annual Conference of IEEE Region 5*, pages 39–43, 2003.

[153] George Voyatzis and Ioannis Pitas. Digital image watermarking using mixing systems. *Computers & Graphics*, 22(4):405–416, 1998.

[154] Josef Scharinger. Secure digital watermark generation based on chaotic Kolmogorov flows. In *Security and Watermarking of Multimedia Contents II*, volume 3971 of *Proceedings of SPIE*, pages 306–313, 2000.

[155] Nikos Nikolaidis, Sofia Tsekeridou, Athanasios Nikolaidis, Anastasios Tefas, Vassilios Solachidis, and Ioannis Pitas. Applications of chaotic signal processing techniques to multimedia watermarking. In *Proc. IEEE workshop on Nonlinear Dynamics in Electronic Systems*, pages 1–7, 2000.

[156] Der-Chyuan Lou, Te-Lung Yin, and Ming-Chang Chang. An efficient steganographic approach. *Computer Systems Science & Engineering*, 17(4/5):263–273, 2002.

[157] Anastasios Tefas, Athanasios Nikolaidis, Nikos Nikolaidis, Vassilios Solachidis, Sofia Tsekeridou, and Ioannis Pitas. Performance analysis of correlation-based watermarking schemes employing Markov chaotic sequences. *IEEE Trans. Signal Processing*, 51(7):1979–1994, 2003.

[158] Franco Chiaraluce, Lorenzo Ciccarelli, Ennio Gambi, Paola Pierleoni, and Maurizio Reginelli. A new chaotic algorithm for video encryption. *IEEE Trans. Consumer Eletronics*, 48(4):838–844, 2002.

[159] Shujun Li, Xuan Zheng, Xuanqin Mou, and Yuanlong Cai. Chaotic encryption scheme for real-time digital video. In *Real-Time Imaging VI*, volume 4666 of *Proceedings of SPIE*, pages 149–160, 2002.