Research Journal of Applied Sciences, Engineering and Technology 7(18): 3791-3796, 2014
DOI:10.19026/rjaset.7.735
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2014 Maxwell Scientific Publication Corp.
Submitted: October 26, 2013 Accepted: December 04, 2013 Published: May 10, 2014

Research Article

A New Approach of Crypto-compression on MPEG Format

Y. Benlcouiri, M. Benabdellah, M.C. Ismaili and A. Azizi
ACSA Laboratory, Faculty of Sciences, Mohammed First University, Oujda, Morocco

Abstract: Issues of security and compression of transmitted data have become an important concern in multimedia technology. In this study, we propose an efficient approach to secure video sequences in real time using the method of choosing reference images that is based on the Faber-schauder Multi-scale Transform to reduce the data flow. The encryption step is based on the principle of affine encryption to achieve transposition and to perform some manipulations such as puzzle to reduce the amount of bits to be processed on the image. Testing this approach on video sequences revealed an improvement in data flow and provides a stronger security and a good encryption time.

Keywords: Compression, congruence, encryption, Faber-schauder Multi-scale Transform (FMT), MPEG, puzzle, reference image, Z/pZ fields

INTRODUCTION

The sharing and the transmission of multimedia documents in various fields (medical, video-conference, IPTV ...) on the computer network have increased. Consequently, the need in cryptography and compression is become inescapable to secure the transmission and minimize the documents size.

Several works around compression have leads to the standards such as H-263, H. 26L and MPEG. The Moving Picture Experts Group (MPEG) compression is one of the most used methods. In Benabdellah *et al.* (2005), the authors have based on the image edge detection in order to optimize the selection of the best reference image. In 2007, Benabdellah *et al.* (2007) applied the Faber-schauder Multi-scale Transform (FMT) on intra and predictive images of each GOP (Group of Pictures) to compare the resulting images after subtraction, in order to choose the optimal one.

Using standard encryption algorithms like Data Encryption Standard (DES), Rivest Cipher (RC5) and Advanced Encryption Standard (AES) do not give a satisfactory solution concerning the video (Zeghid *et al*., 2007). In fact, the application of these algorithms, even on compressed shape, is confronted by the constraint of time required to encrypt/decrypt.

Many research efforts have been devoted to encrypt/decrypt video in real time has been done. Tang (1996) is based on the scrambling principle by permutation of the DCT coefficients of each macro-block separately. The idea is using a random permutations list, to replace the zig-zag order of the DCT coefficients of a block to a 1×64 vectors. Zeng and Lie (2003) proposed an extension of Tang algorithm operating, not on the macro-blocks, but on segments, each one consisting of macro-blocks. They permute the set of DCT coefficients of each segment separately from the other, for each intra frame of a GOP and also, they permute the motion vectors of P and B frames. Choon (2004) proposed a fast encryption algorithm based on confusion/diffusion principle introduced by Shannon (1949). It consists on macro-blocks permutation in order to perform the diffusion, afterwards, XOR operations to make confusion. Choo *et al.* (2007) have introduced a Crypto-system for uncompressed raw MPEG data, called Secure Real-time Media Transmission (SRMT), by using two transposition steps and one of XOR operation. In 2013, Benlcouiri *et al.* (2013) have presented a randomized encryption method, which is based on the puzzle principle and the extended affine cipher on field $\mathbb{Z}/p\mathbb{Z}$ to scramble the puzzle. The advantages of this method are its randomness concerning the choice of key as well as the execution time which is proportional to the number of puzzle pieces. We exploit the speed of this method to meet the operational needs of encryption/decryption, especially, in the video conference, live-tv, VoD, IPTV, etc. However, light-weight encryption and scramble-only methods provide less security than the naive encryption.

In this study, we propose a new Crypto-compression approach for MPEG format based on FMT and the extended affine cipher. It encrypts only I-frame selected by using the Faber-schauder Multi-scale Transform. The main advantages of this approach are flexibility, reduction of data flow and processing time, which is proportional to the number of puzzle pieces during the operation of encryption/decryption. Indeed, through this method we can vary the processing time depending on the desired level of security.

Corresponding Author: Y. Benlcouiri, ACSA Laboratory, Faculty of Sciences, Mohammed First University, Oujda, Morocco
This work is licensed under a Creative Commons Attribution 4.0 International License (URL: http://creativecommons.org/licenses/by/4.0/).

The body of the present study will be organized as follow. In the second section, we present the Structure of Coding MPEG Format, describe the FMT wavelet transform and we expose the affine cipher method. The third one is devoted to our new crypto-compression approach. Then, we will describe in detail a results obtained after its implementation. Finally we conclude this study by introducing some perspectives.

METHODOLOGY

Structure of coding MPEG format: The MPEG standard defines a set of coding stages that transform a video signal (digitized in standardized format) into a binary stream (a bit stream) intended to be stored or transmitted through a network. The binary stream is described according to a syntax coded in a standardized way that can be restored easily by any decoder that recognizes the MPEG standard. The coding algorithm defines a hierarchical structure containing the levels described in the following Fig. 1 (Benabdellah *et al.*, 2007).

The group of pictures or GOP consists of a periodic continuation of compressed images. There are three types of the compressed images: Intra image (I) compressed using JPEG for the fixed images, Predictive image (P) coded using a prediction of a previous image of type I or P and Bidirectional image (B) coded by double prediction (or Interpolation) by using a previous image of type I or P and a future Intra image or Predictive image as references. A GOP starts with an image I, contains a periodic continuation of the images P separated by a constant number of images B as in the following Fig. 2. The structure of GOP is thus defined by two parameters: the number of images of GOP and the distance between Intra images and Predictive image.

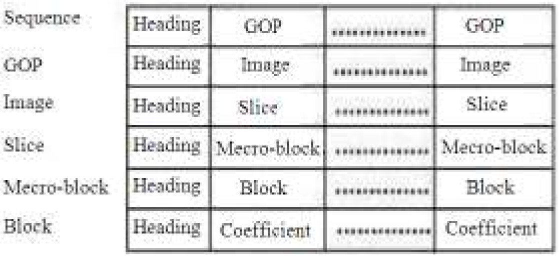
Faber-schauder Multi-scale Transform (FMT): The Faber-Schauder wavelet transform is a simple multi-scale transformation with many interesting properties in image processing. In these properties, we advertise multi-scale edge detection, preservation of pixels ranges, elimination of the constant and the linear correlation.

For the construction of the Faber-Schauder base, we suppose the family of under spaces $(W_j)_{j\in Z}$ of L^2 (R^2) such as V_j is the direct sum of V_{j+1} and $W_{j+}1$ (Benabdellah *et al.*, 2007):

$$V_j = V_{j+1} \oplus W_{j+1}$$
$$W_{j+1} = (V_{j+1} \times W_{j+1} \oplus W_{j+1} \times V_{j+1} \oplus W_{j+1} \times W_{j+1})$$

The space base W_{j+1} is given by:

$$(\psi^{j+1}_{1,k,l} = \varphi^{j}_{2k+1} \times \psi^{j+1}_{l}, \psi^{j}_{2,k,l} = \psi^{j+1}_{k} \times \varphi^{j}_{2l}, \psi^{j}_{3,k,l} = \psi^{j+1}_{k} \times \psi^{j+1}_{l})_{k,l\hat{I}Z}$$



Sequence	Heading	GOP	....	GOP
GOP	Heading	Image	....	Image
Image	Heading	Slice	....	Slice
Slice	Heading	Mecro-block	....	Mecro-block
Mecro-block	Heading	Block	....	Block
Block	Heading	Coefficient	....	Coefficient

Fig. 1: Hierarchical structure of MPEG coding

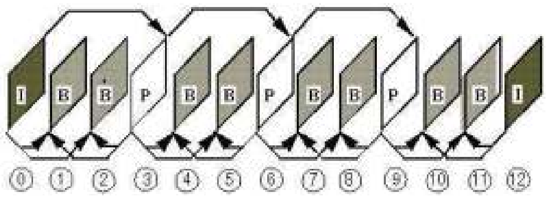


Fig. 2: Structure of GOP

The unconditional base and Faber-Schauder multi-scale of L^2 (R^2) is given by:

$$(\psi^{m}_{1,k,l}, \psi^{m}_{2,k,l}, \psi^{m}_{3,k,l})_{k,l,m\in Z}$$

A function of V_0:

$$f(x,y) = \sum_{k,l\in Z} f^{0}_{k,l}\varphi^{0}_{k,l}(x,y)$$

Can be broken up in a single way according to V_1 and W_1 (Benabdellah *et al.*, 2007):

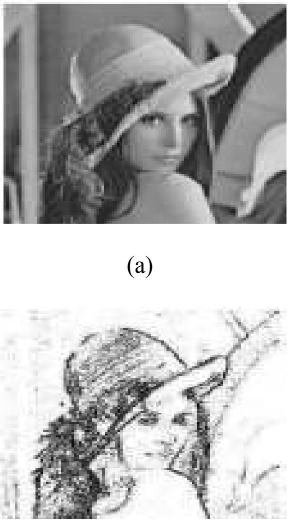
$$f(x,y) = \sum_{k,l\in Z} f^{1}_{k,l}\varphi^{1}_{k,l}(x,y)$$
$$+\sum_{k,l\in Z}[g^{11}_{k,l}\psi^{1}_{k,l}(x,y) + g^{21}_{k,l}\psi^{2}_{k,l}(x,y) + g^{31}_{k,l}\psi^{3}_{k,l}(x,y)]$$

The continuation f^1 is a coarse version of the original image f^0 (a polygonal approximation of f^0), while $g^1 = (g^{11}, g^{21}, g^{31})$ represents the difference in information between f^0 and f^1. g^{11} (respectively g^{21}) represents the difference for the first (respectively the second) variable and g^{31} the diagonal represents difference for the two variables (Benabdellah *et al.*, 2007).

The continuations f^1 and g^1 can be calculated starting from f^0 in the following way:

$$f^{1}_{k,l} = f^{0}_{2k,2l}$$
$$g^{11}_{k,l} = f^{0}_{2k+1,2l} - 1/2(f^{0}_{2k,2l} + f^{0}_{2k+2,2l})$$
$$g^{21}_{k,l} = f^{0}_{2k,2l+1} - 1/2(f^{0}_{2k,2l}) + f^{0}_{2k,2l+2})$$
$$g^{31}_{k,l} = f^{0}_{2k+1,2l+1} - 1/4(f^{0}_{2k,2l} + f^{0}_{2k,2l+2} + f^{0}_{2k+2,2l} + f^{0}_{2k+2,2l+2})$$

Reciprocally one can rebuild the continuation f^0 such as $f^{0}_{2k,2l}$, $f^{0}_{2k+1,2l}$, $f^{0}_{2k,2l+1}$ and $f^{0}_{2k+1,2l+1}$ from f^1 and g^1 by the four relationships indicated above.



(a)

(b)

Fig. 3: Representation on mixed-scales and separate scales of the image “lena”, the coefficients are in the canonical base, (a) and in the faber-schauder multi-scale base (b)

We can consider the FMT multi-scale transformation as a linear application, from the canonical base to the multi-scale base, which distributes the information contained in the initial image in a different way. It is thus more natural to visualize this redistribution, in the multi-scale base, in only one image, as it is the case in the canonical base. The principle of the visualization of images in the canonical base consists in placing each coefficient at the place where its basic function reaches its maximum. The same principle is naturally essential for the multi-scale base.

The image obtained is a coherent one which resembles an outline representation of the original image (Fig. 3). Indeed, the FMT transformation, like some wavelets transformation, has similarities with the canny outlines detector, where the outlines correspond to the local maximum in the module of transformation. In fact, in the case of the FMT transformation, on each scale, the value of each pixel is given by the calculation of the difference with its neighboring of the preceding scale. Thus the areas which present a local peak for these differences correspond to a strong luminous transition for the values of grey, while the areas, where those differences are invalid, are associated with an area, where the level of grey is constant (Benabdellah *et al*., 2007).

Encryption: The most methods of encryption based on two principles: substitution and transposition. Substitution means that replacing some letters by symbols or others. Transposition means that permuting the letters of the message to make it unintelligible. Over the centuries, many systems of cryptographic Telecare Medicine Information System (TMIS) have developed more perfection more clever (Benlcouiri *et al*., 2013).

Congruence: For u, v in Z and n an integer ≥2, the notation $u \equiv v \bmod(n)$ reads u congruent to v modulo n and means that $(u - v)$ is divisible by n which is equivalent to say that u and v have the same retained when divided by n, for example 17 = 5 (3) but also -1 = 1 (2). (Benlcouiri *et al*., 2013):

u, v, r, s belong to $\mathbb{Z}$ and n an integer ≥2
if $u \equiv v$ (n) and $r \equiv s$ (n) so:
$u + r \equiv v + s$ (n); $u-r \equiv v-s$ (n); $u\times r \equiv v\times s$ (n)
and for all k Є $\mathbb{Z}$ we have $u \equiv v + kn$ (n)
if u and v are two integers belonging to {0; 1; 2;… n-1}
so $u \equiv v$ (n) implies $u \equiv v$

The extended euclidean algorithm: The extended Euclidean algorithm permits to calculate the inverse of b modulo n if it exists. Remembering that the inverse of modulo n of b is the whole number b^{-1} such that $b\times b^{-1} = 1$ (mod n) for example 7 is the inverse modulo 9 of 4 because 4×7 = 28 = 1 (mod 9):

Algorithm:

```
$n_0$ : = n
$b_0$ : = b
$t_0$ : = 0
t : = 1
q : =  an integer less than or equal to $n_0/b_0$
r : = $n_0$ - q×$b_0$
  while r>0 do
   start
     temp : = $t_0$ - q×t
     if temp > = 0 then
      temp : = temp mod n,
      else temp : = n - ((-temp) mod n)
          $t_0$ : = t
          t : = temp
          $n_0$ : = $b_0$
          $b_0$ : = r
          q : = an integer less or equal to $n_0/b_0$
          r : = $n_0$ - q×$b_0$
  end while;
if $b_0 \neq 1$ then b has no inverse modulo n,
else $b^{-1}$ mod n = t
```

This algorithm can also calculate the Bezout coefficients of a and b, (called extended Euclidean algorithm). Recalling that if d is the Greatest Common Divisor (GCD) of a and b, there exists the whole u and v such that $au + bv = d$. The Euclidean algorithm allows calculating these u and v coefficients. Simply go up the calculations by expressing the GCD d as a function of other numbers (Benlcouiri *et al*., 2013).

Affine encryptions: Noting that E = {0; 1; 2… 25}, a and b are integers selected from E. Coding is affine, after numbered from 0 to 25 letters of the alphabet, to encode a letter (called source) number x by the letter number y, where y is the remainder of the division of $\mathrm{ax} + \mathrm{b}$ by 26. The encoding function associated affine associated with the coefficients a and b is the function f from E to E in which x matches to $\mathrm{f}(\mathrm{x}) = \mathrm{y}$. f (x) is the only element of the set E = {0, 1, 2... 25} which is congruent to $\mathrm{ax} + \mathrm{b}$ modulo 26, $\mathrm{f}(\mathrm{x}) \equiv \mathrm{ax} + \mathrm{b} \bmod (26)$ (Benlcouiri *et al*., 2013).

Proposed method: The proposed method includes two steps: compression step and encryption step.

The compression step: Consists in extracting the various images initially; Intra image, Predictive image and Bidirectional image constituting the video sequence.

We apply the FMT only on Intra and Predictive images. Then, we make the subtraction between the resulting images. We choose the best reference image for each image as follows:

- If we will have results, after subtraction of resulting images, containing only the points, we choose the best reference image for the concerned image, that which corresponds to the result containing the minimum number of points.
- If we will have results containing the points and the parallel linear or nonlinear curves. We choose the best reference image for the concerned image that which corresponds to the result containing the minimal distance between parallel linear or nonlinear curves.

The encryption: Step consists in encrypting only Intra pictures in each GOP of MPEG sequence while keeping the motion vectors responsible for reconstruction of the P images and the B images. It is to use the principles of an affine encryption on field type $\mathbb{Z}/\mathrm{p}\mathbb{Z}$ married to the results of modular arithmetic and the problem of the puzzle to complete the transposition of elements.

The keys generation: For our method is divided into three parts:

- Choose a prime number p to work on the $\mathbb{Z}/p\mathbb{Z}$ field, in which all elements are invertible.
- Subdivide the image processing into $p-1$ puzzle pieces (square, triangle…) with ($n\times n$) blocks size according to the required security level.
- Select a pair of elements (a, b) in $[(\mathbb{Z}/p\mathbb{Z})^*, (\mathbb{Z}/p\mathbb{Z})]$ and calculate the inverse of a using the extended Euclidean algorithm: $a \times a^{-1} \equiv 1 mod\ (p)$.

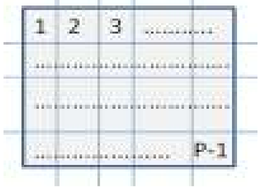


Fig. 4: Original intra image divided into (p-1) macro-blocks

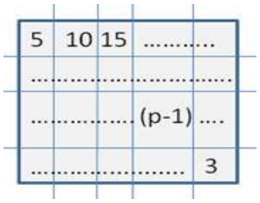


Fig. 5: Encrypted image after transposition of (p-1) macro-blocks

The encryption key is threefold: $[p; (a, b); (n, m)]$ and the decryption key is $[p; (a^{-1}, b); (n, m)]$.

Encryption step: We divide each image Intra of each GOP of the MPEG video sequence in (p-1) macro-blocks as shown in the following Fig. 4.

After subdividing the Intra image in $(p-1)$ macro-blocks numbered from 1 to p-1, we proceed as following.

Let f be the mapping defined as follows:

$$f: \mathbb{Z}/\mathrm{p}\mathbb{Z} \rightarrow \mathbb{Z}/\mathrm{p}\mathbb{Z}$$
$$x \rightarrow ax + b\ mod(p)$$

To change the location of each macro-block of image processing, we apply the function f to its indices:

$$\{f(1);\ \ldots .f(p-1)\} = \{5; (p-1); \ldots 3\}_{transpose}$$

Reorganize the results after applying the function f on the indices of macro-blocks conducted a transposition. The encrypted image is shown in the Fig. 5.

Reconstruct the video sequence by replacing the original Intra image by the Intra image after processing.

Decryption step: The decryption key is the triple $[\mathrm{p}; (\mathrm{a}^{-1}, \mathrm{b}); (\mathrm{n}, \mathrm{m}); \mathrm{L}]$, when L is the index of the new reference image.

We perform the extraction of images number L on the video sequence encrypted then remake the same calculation performed in the encryption phase to find the order of transposition using f.

We rearrange the encrypted image according to the result obtained:

$$\{5; 10; \ldots; (p-1); \ldots 3\}_{transpose}$$

Then we apply the MPEG algorithm for the decoded video sequence.

APPLICATION AND RESULTS

For apply the proposed method we process as follows:

- Extract still images that constitute the video sequence
- Application of the FMT on the Intra and Predicted images. Next, make the extraction from the resulting images. Then use the two criteria we proposed to select the best reference image for each image (Intra and Predictive)
- Now, for each Intra image we proceed as follows: We choose a prime number p = 257 to work on the fields ℤ/pℤ =ℤ/257ℤ
- Then we divide the image into (p-1) = 256 elements each of size (n × m) where n = 8 and m = 8
- We selected from (ℤ/257ℤ) the pair (a, b) = (195, 10) that we have used, by applying the function f to bring the biggest mess possible

The decryption key is the same as the encryption and it is given as follows:

K = [257; [(195, 10); (8×8)]

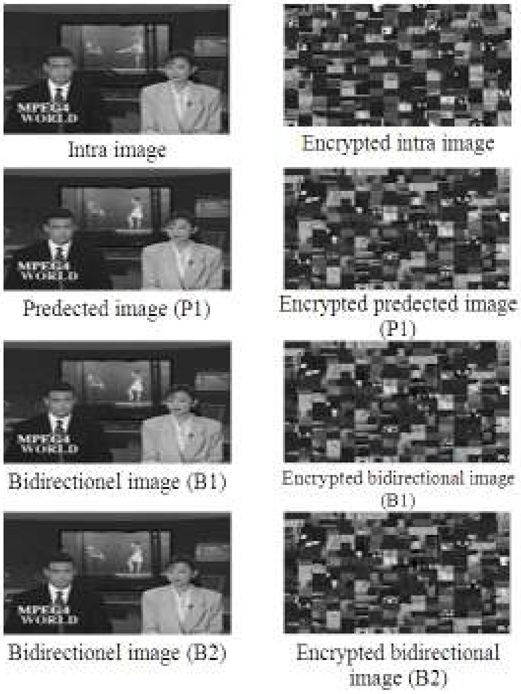
The results of our method application using the key K are illustrated in the Table 1 and Fig. 6.

We notice that this introduced method concerns the reduction of information for a minimal storage and a transmission by reduced flow because after application of the step of choosing the right reference images, the GOP is rearranged: The image I became the image P3, the image P1 became the image I, the image P2 became the image P1 and the image P3 became the image P2.

After reconstruction of the new sequence, the entropy of the original Intra image is equal to that of the encrypted Intra image which provides a high degree of security (Fig. 6) according to law of security measure that is introduced by Shannon in information theory. The entropy of the Encrypted Images P1, B1 and B2 is a little higher than that of the original images P1, B1 and B2 (Table 1).

The subdivision of the image into 256 macro-blocks allows us, on encryption, to make a calculation of codes into 8 bits and obtain a minimum processing time.

We separately encrypted the Intra image whose computation time was 2 (ms). Then, we applied the MPEG algorithm to reconstruct the images P and B who are encrypted with computation time equal to 0. Also, by our approach we have obtained a memory of the encrypted GOP smaller than the memory of original GOP (Table 1).



Intra image

Encrypted intra image

Predected image (P1)

Encrypted predected image (P1)

Bidirectionel image (B1)

Encrypted bidirectional image (B1)

Bidirectionel image (B2)

Encrypted bidirectional image (B2)

Fig. 6: Encryption intra image and its effect on P and B images of news sequence (GOP (1: 12))

Table 1: Results after applying our method on intra image

Our method					
GOP (1:12)	E.O.I	E.E.I	E.T (ms)	MCO (ko)	MCE (ko)
Intra image	7.0675	7.0675	2		
Predictive image (P1)	7.0005	7.0834	0.00	4.44	4.41
Bidirectional image (BI)	6.9285	7.2061	0.00		
Bidirectional image (B2)	6.9199	7.2807	0.00		

E.O.I: Entropy of original image; E.E.I: Entropy of encrypted image; E.T: Encryption time (ms); M.C.O: Memory capacity of the GOP-MPEG original; M.C.E: Memory capacity of the encrypted GOP-MPEG

CONCLUSION

We introduced an encryption-compression approach of video sequences based on the FMT and the affine encryption. The encryption step by the affine encryption enabled us to produce a method of transposition on field (ℤ/pℤ) use of the principle of the puzzle allows to reduce the amount of pixels processed the results obtained from our application, shows that the complexity can produce such a system of transposition.

The main idea behind this study is to carry out tests on the modification of the encoding sequence of the video sequence images to produce a gain in the result.

Some tests highlighted a possible gain for certain sequences through the choice of the reference images. The FMT transformation is distinguished by its simplicity and its performances of seclusion of the information in the out-line regions of the image. The mixed-scale visualization of the transformed images allows putting in evidence its properties, particularly, the possibilities of compression of the images and the improvement of the performances of the other standard methods of compression as JPEG and GIF.

Based on its encryption speed and the degree of security it provides, we want to marry the encryption step with other compression methods to produce new encryption-compression approaches of video and still images.

ACKNOWLEDGMENT

Supported by the Hassan II Academy of science and technology of Morocco.

REFERENCES

Benabdellah, M., M. Gharbi, F. Regragui and E.H. Bouyakhf, 2005. A method for choosing reference images based on edge detection for video compression. Georgian Electron. Sci. J. Comput. Sci. Telecommun., 3(7): 33-39.

Benabdellah, M., M. Gharbi, F. Regragui and E.H. Bouyakhf, 2007. Choice of reference images for video compression. Int. J. Appl. Math. Sci., 1: 2187-2201.

Benlcouiri, Y., M. Benabdellah, M.C. Ismaili and A. Azizi, 2013. Affine cipher extended to (Z/pZ) and it's application in images. Proceedings of the 20th International Conference on Telecommunications (ICT, 2013), pp: 1-5.

Choo, E., J. Lee, H. Lee and G. Nam, 2007. SRMT: A lightweight encryption scheme for secure real-time multimedia transmission. Proceedings of the International Conference on Multimedia and Ubiquitous Engineering, pp: 60-65.

Choon, L.S., 2004. Lightweight and cost-effective MPEG video encryption. Proceedings of the International Conference on Information and Communication Technologies: From Theory to Applications, pp: 525-526.

Shannon, C.E., 1949. Communication theory of secrecy systems. Bell Syst. Tech. J., 28: 656-715.

Tang, L., 1996. Methods for encrypting and decrypting MPEG video data efficiently. Proceedings of the 4th ACM International Conference on Multimedia, pp: 219-229.

Zeghid, M., M. Machhout, L. Khriji and A. Baganne, 2007. A modified AES based algorithm for image encryption. Int. J. Comput. Sci. Eng., 1(1): 70-75.

Zeng, W. and S. Lei, 2003. Efficient frequency domain selective scrambling of digital video. IEEE T. Multimedia, 5: 118-219.