

PROCEEDINGS OF SPIE

SPIDigitalLibrary.org/conference-proceedings-of-spie

Efficient encryption of image data in video sequences using discrete orthogonal moments

J. S. Rivera-López
C. J. Camacho Bello

SPIE.

Efficient encryption of image data in video sequences using discrete orthogonal moments

J.S. Rivera-López, C.J. Camacho Bello
Universidad Politécnica de Tulancingo(México),

ABSTRACT

Currently, new techniques have been implemented to provide data security, confidentiality, integrity and authentication. Orthogonal moments can be used for the watermark in small binary images. In this work we use this principle to encrypt a grayscale image in a video sequence. To validate our approach, we present a comparative analysis using different families of discrete orthogonal moments in terms of accuracy. Finally, results and conclusions are presented.

Keywords: encryption of image, discrete orthogonal moment, Tchebichef, Krawtchouk and Charlier polynomials, video sequence, image recovery.

1. INTRODUCTION

Lately, discrete orthogonal moments have been used in different research areas, such as: image registration [1], face recognition [2], angle of estimation [3], watermark [4], patterns of Reconstruction [5], medical imaging [6], focal measurements [7], image analysis [8], forensic applications [9], phase-detection gait [10], among others, due to their ability to Represent global characteristics of an image by a set of descriptors, independent of each other, with a minimum amount of information redundancy [11].

In particular, digital watermark technology is considered as a solution to preventing misuse of information. In the last decade watermarking algorithms have been proposed to protect the copyright of multimedia objects such as digital images, audio clips and videos. Different algorithms have been developed for watermarking images in recent years; both spatial and frequency domains are used for watermark embedding. However, the amount of digital multimedia production has been exponentially growing along their vulnerability, also increasing the need for better and more advanced techniques for watermarking digital media objects [12].

The rapid growth in digital multimedia technologies has brought much attention to the field of digital authentication. The digital watermark has been widely recognized as an effective measure to protect multimedia data copyrights [18].

The digital watermark is an information concealment technique, its main objective is to track the illicit use of certain digital services by unauthorized users. Specifically, this technique consists of inserting a message (hidden or not) into a digital image.

Two major types of digital watermarking techniques are known [19]:

- One type involves the modification of some component in the spatial domain, is easy to implement, BUT is fragile in the face of attacks.
- The second type involves modification of some component in the transformed frequency domain, is complex to implement, but robust in the event of modifications, which should not be ambiguous.

There has been research on watermarks and their creation using orthogonal functions [13], orthogonal moments [14, 15,16] and sine transformation [16,17], among others.

In this paper, an algorithm is presented, which allows encryption and decryption of a grayscale image in a video sequence through the use of discrete orthogonal moments in order to protect information and provide greater security and confidentiality of same. Also, the video can be marked with a hidden copyright image with the possibility of showing the results obtained when encrypting test images in a video and the recovery of the encrypted image. Recovery also allows us to see the reconstruction errors using the discrete orthogonal moments of three different families of orthogonal polynomials.

2. DISCRETE ORTHOGONAL MOMENTS

The discrete orthogonal moments are scalar quantities used to describe an image and describe its most important characteristics, which has as A kernel a base of discrete orthogonal polynomials [20].

The orthogonal moments are defined as follows:

$$\phi_{m,n} = \sum_{x=1}^m \sum_{y=1}^n f(x,y)P_n(x)P_m(y) \quad (1)$$

where $P_n(x)$ and $P_m(y)$ are a set of discrete orthogonal polynomials AND $f(x,y)$ is an image function.

It is possible to reconstruct an image from its moments, using the respective inverse transform. The reconstruction of an image $f(x,y)$ is given by:

$$\tilde{f}(x,y) = \sum_{x=1}^M \sum_{y=1}^N \phi_{m,n}P_n(x)P_m(y), \quad (2)$$

where $P_n(x)$ and $P_m(y)$ are polynomial basis functions and $M_{m,n}$ are the moments of the image to be reconstructed. Hence, the moments of an image can be used to encrypt information and, through reconstruction, TO retrieve the original image with hidden information.

2.1. Discrete orthogonal polynomials

The discrete polynomials of orthogonal bases used for the calculation of moments have their origin in the polynomial solutions of the following finite DIFFERENCE equation [21]:

$$\sigma(x)\Delta \nabla p_n(x) + \tau(x)\Delta p_n(x) + \lambda_n p_n(x) = 0, \quad (3)$$

where $\Delta p_n(x) = p_n(x+1) - p_n(x)$, and $\nabla p_n(x) = -p_n(x) - p_n(x+1)$, denote the forward and backward operator in finite differences, respectively; λ_n is an appropriate constant; $\sigma(x)$ and $\tau(x)$ are first and second degree functions of any family of orthogonal polynomials, respectively. For classical orthogonal polynomials, the functions $\sigma(x)$ and $\tau(x)$ and the constant λ_n are different for each family. The parameters of the classical polynomials are shown in Table 1.

Parameters	$t_n(x; N)$	$k_n(x; p, N)$	$c_n^{a_1}(x)$
$\sigma(x)$	$x(N-1)$	x	x
$\tau(x)$	$N-1-2x$	$\frac{Np-x}{(1-p)}$	a_1-x
λ_n	$n(n+1)$	$\frac{n}{1-n}$	n

Table 1: Functions $\sigma(x)$, $\tau(x)$ and λ_n of the following functions: Tchebichef $t(x; N)$, Krawtchouk $k(x; p, N)$ and Charlier $c_n^{a_1}(x)$.

A general way to obtain normalized discrete orthogonal polynomials $\tilde{p}_n(x)$ is by the following recurrence relation (H. Zhu et al [22]).

$$A\tilde{p}_n(x) = B * D\tilde{p}_{n-1}(x) + C * E\tilde{p}_{n-2}(x) \quad (4)$$

where A, B, C, D, E are terms independent of each of the polynomial families mentioned and $\tilde{p}_{n-1}(x), \tilde{p}_{n-2}(x)$. The initial values in Table 2.

	$\tilde{t}_n(x; N)$	$\tilde{k}_n(x; p, N)$	$\tilde{c}_n^{a_1}(x)$
$\tilde{p}_0(x)$	$\frac{1}{\sqrt{N}}$	$\sqrt{\frac{N! p^x (1-p)^{N-x}}{x! (N-x)!}}$	$\sqrt{\frac{e^{-\mu} \mu^x}{x!}}$
$\tilde{p}_1(x)$	$(N-1-2x) \sqrt{\frac{3}{N(N^2-1)}}$	$* \sqrt{\frac{-p(N-x) + x(1-p)}{(N-1)! p^{x-1} (1-p)^{N-x-1} x! (N-x)!}}$	$\frac{\mu-x}{\mu} \sqrt{\frac{e^{-\mu} \mu^{x+1}}{x!}}$
A	$\frac{n}{2(2n-1)}$	n	$-a_1$
B	$x - \frac{N-1}{2}$	$x - n + 1 - p(N - 2n + 2)$	$x - n + 1 - a_1$
C	$-\frac{(n-1)(N^2 - (n-1)^2)}{2(2n-1)}$	$-p(1-p)(N-n+2)$	$n-1$
D	$\sqrt{\frac{(2n+1)}{(N^2 - n^2)(n+1)}}$	$\sqrt{\frac{n}{p(1-p)(N-n+1)}}$	$\sqrt{\frac{a_1}{n}}$
E	$\sqrt{\frac{(2n+1)}{(N^2 - n^2)(N^2 - (n+1))(2n-3)}}$	$\sqrt{\frac{n(n-1)}{p(1-p)(N-n+2)(N-n+1)}}$	$\sqrt{\frac{a_1^2}{n(n-1)}}$

Table 2: Polynomials of order zero and one and terms A, B, C, D and E of the following functions: Tchebichef $\tilde{t}_n(x; N)$, Krawtchouk $\tilde{k}_n(x; p, N)$ y Charlier $\tilde{c}_n^{a_1}(x)$.

Below are the graphs of the first 10 polynomials of the polynomials in Table 1.

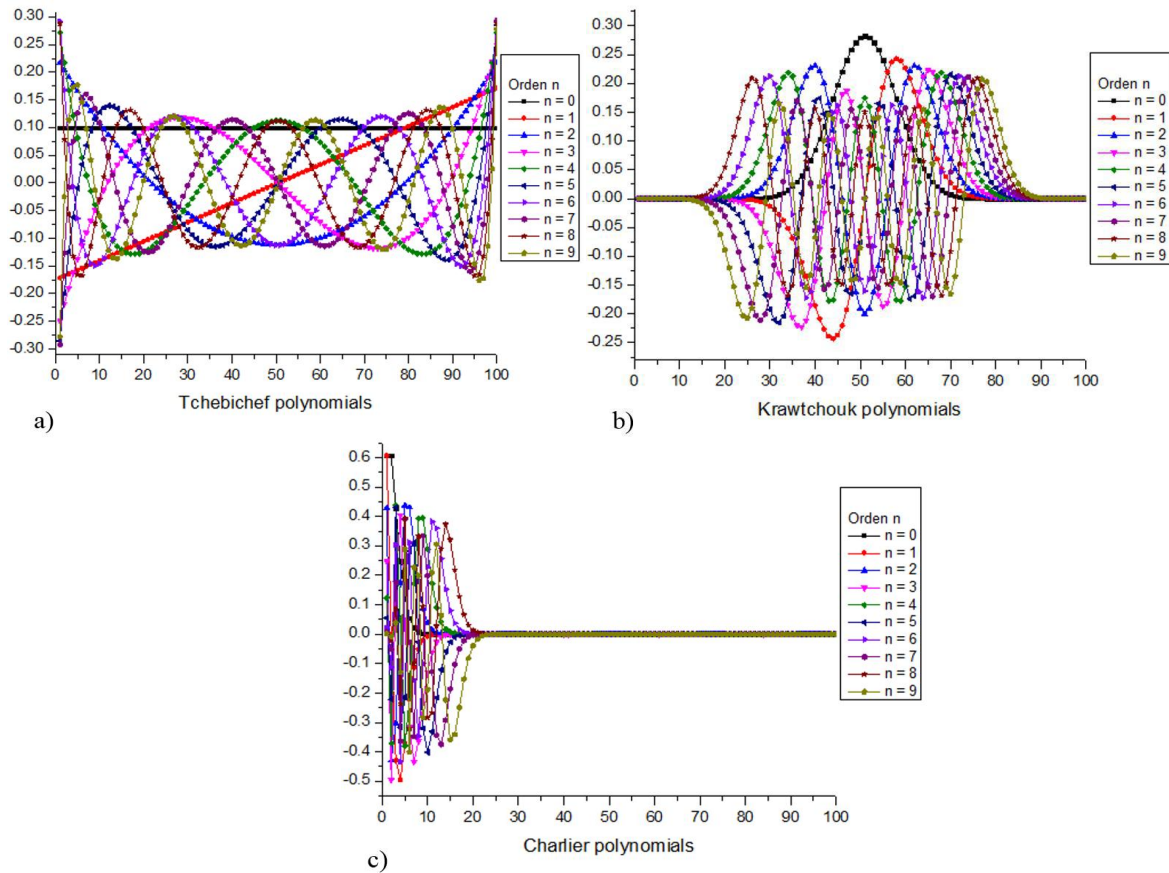


Figure 1. The first ten polynomials $n=0,1,2, \dots, 9$. a) Tchebichef polynomials, b) Krawtchouk polynomials, and c) Charlier polynomials.

3. PROPOSED ALGORITHM TO ENCRYPT AN IMAGE IN A VIDEO

Most studies related to information encryption refer to the insertion of a watermark into an image. This paper proposes an algorithm that allows image encryption in a video. The process can be defined as a sequence of images presented at a certain rate expressed in the number of frames per second (FPS).

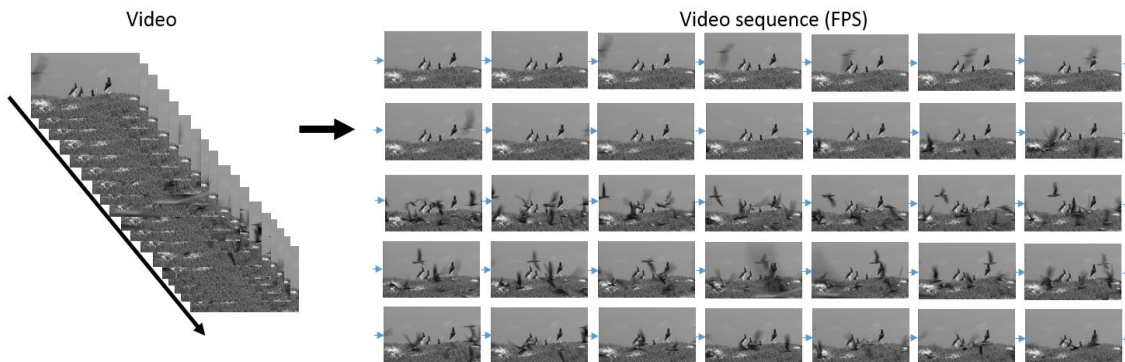
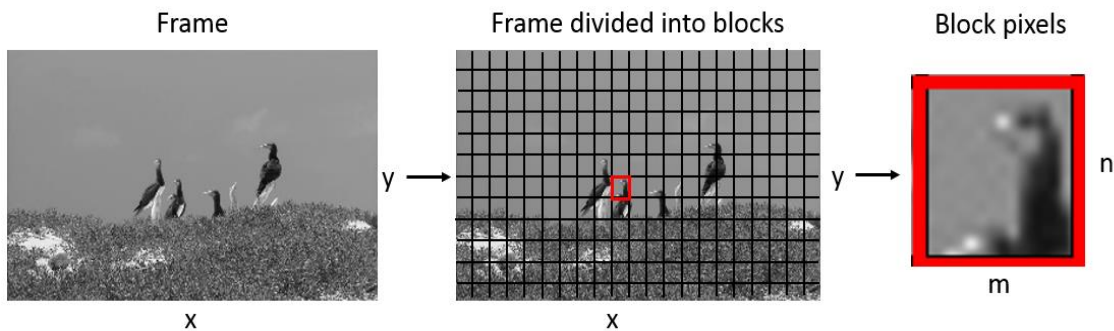


Figure 2. Picture of a video sequence.

The algorithm begins by taking the first frame $f(x, y)$ of the video sequence and divides it into blocks of $n \times m$.



3. Picture of a video sequence divided into blocks.

Similarly, the algorithm divides the image by encrypting $g(M, N)$ into blocks of $i \times j$ with a ratio of $i = M/8 * m$ y $j' = N/n$, which contain the intensity values of the image to be encrypted. Once the image block is obtained, the algorithm converts each intensity level of the block to its binary number equivalent, yielding a matrix I .

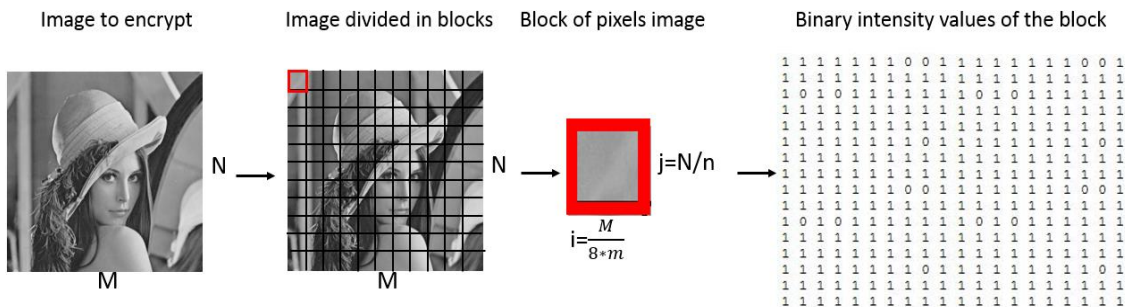


Figure 4. Obtaining the Binary Value Matrix

The algorithm then calculates the moments of each block of the divided image shown in Fig. 3.

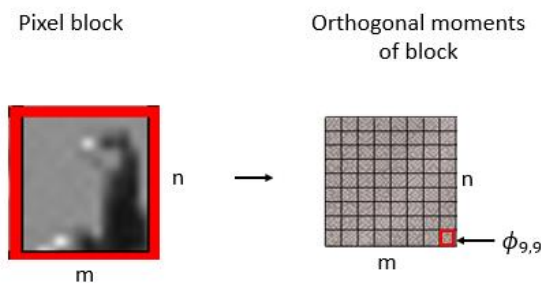


Figure 5. Calculation of moments of the image.

To insert each binary value of matrix I into the block of the video frame, the condition shown in Fig.6 is used, which is necessary to establish a threshold value v that allows image encryption and recovery.

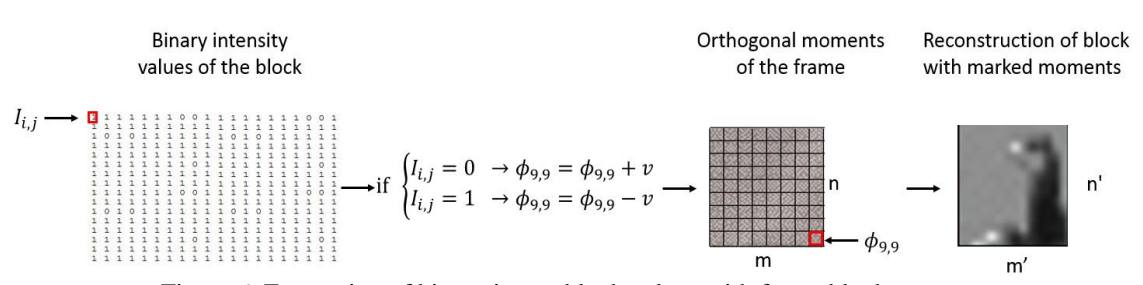


Figure 6. Encryption of binary image block values with frame block moments.

Finally, the algorithm serves to reconstruct each block with the marked moments and return the blocks to their original position, so that we get the video frame again but with a part of the encrypted image.

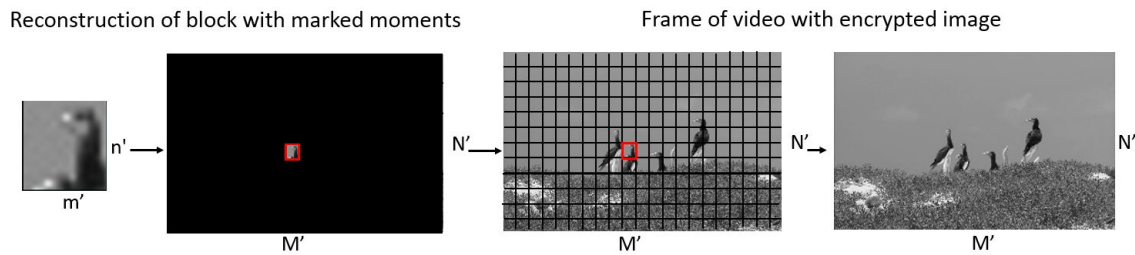


Figure 7. Reconstruction of blocks with the information of the matrix I encrypted.

Once the first frame of the video is finished, the same process is repeated for the following frames. The number of frames used is equal to the number of blocks IN the image to be encrypted

3.1. Recovering the encrypted image

The algorithm for recovering the encrypted image can be considered as reverse image encryption, but here using the video with the encrypted image.

It starts in the same way with the first frame of the video image sequence bearing information on the encrypted image for subsequent block division. Next, moments of each block are calculated, as shown in Fig.8.

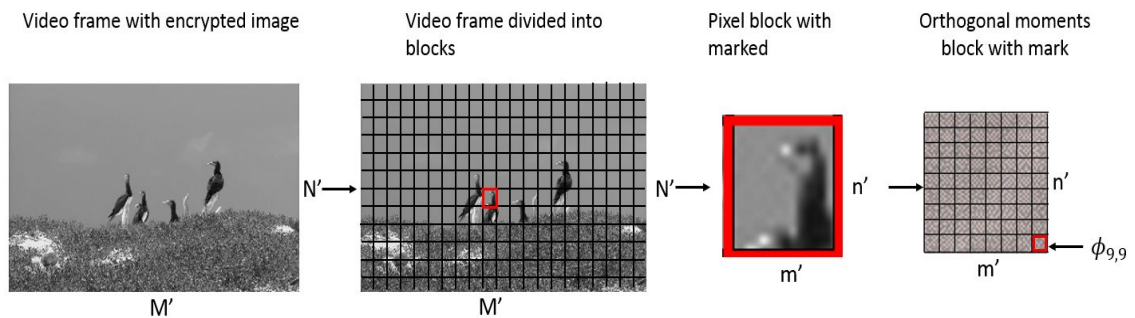


Figure 8. Division of blocks and calculation of moments of the video frame with the encrypted image.

In order to recover the encrypted image, we recover the binary values of the encrypted image intensity values by using the moments of each block as well as a new condition (Fig. 9) that allows us to retrieve the values of each block from the recovered binary matrix I' .

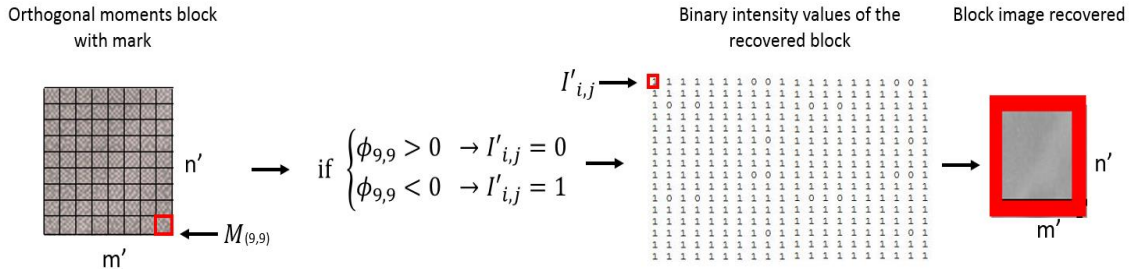


Figure 9. Recover Image Blocks.

Finally, the algorithm retrieves and places each block in the correct position to result in the image AS in Fig. 10.

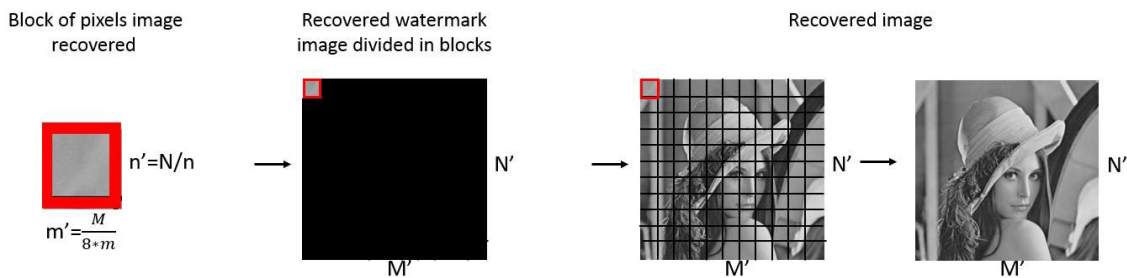


Figure 10. Union of blocks and recovery of the encrypted image.

4. RESULTS OBTAINED

To evaluate the efficiency of the moments, the reconstruction metric based on the Reconstruction Mean Square Error (RMES) is used, which is defined as the normalized square error between the input image $f(x, y)$ and the reconstructed image $\tilde{f}(x, y)$, expressed as:

$$RMES = \frac{\sum_{y=1}^N \sum_{x=1}^M [f(x,y) - \tilde{f}(x,y)]^2}{\sum_{y=1}^N \sum_{x=1}^M f^2(x,y)} \quad (5)$$

where $f(x, y)$ is the original image and $\tilde{f}(x, y)$ is the image retrieved.

Next are the results obtained with the proposed algorithm for video encryption and recovery of the following three grayscale test images with dimensions of 512 x 512 pixels presented in Fig. 11.

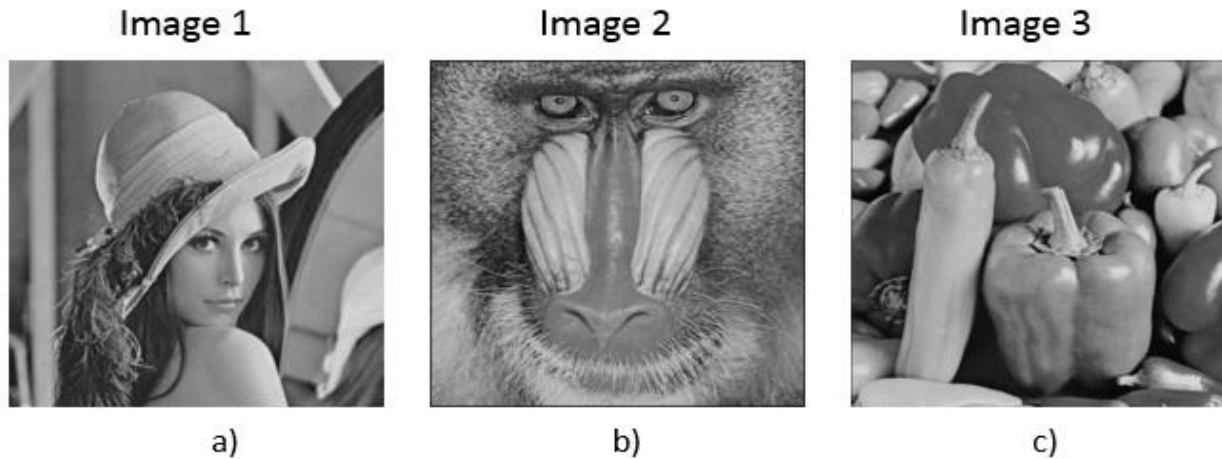


Figure 11. Grayscale image of 512 x 512 used as images for video encryption a) "lena.jpg", b)"mandril.jpg" and c)"pimiento.jpg".

The video that was used is called "wildlife.wmv" or "Natura.wmv", which is A default in Windows 7 (2008 Microsoft) with dimensions of 1280 x 720 pixels AT 30 fps with a duration of 30 Seconds and a total of 900 fps in gray scale.

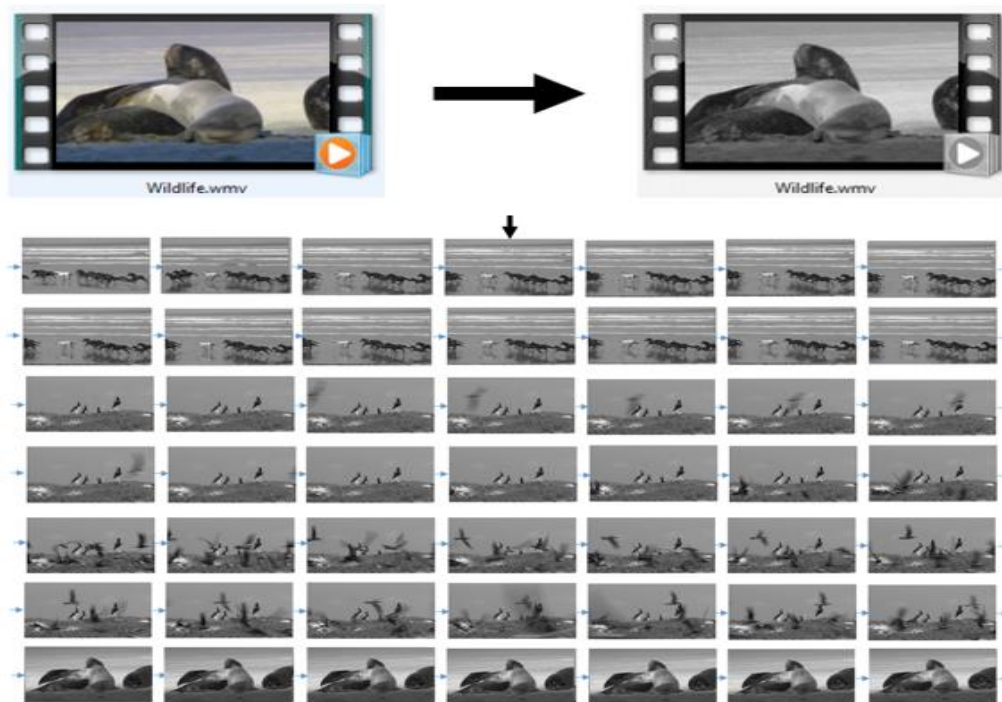


Figure 12. Video in grayscale, from 2008 Microsoft Corp. to encrypt test images.

The encryption of the three test images shown in Fig. 11 was performed with Tchebichef, Krawtchouk, and Charlier moments for the value $v = 50$. A video was obtained for each image used for comparative RMES. In addition, the results obtained with the proposed algorithm are shown in Tables 3, 4, 5.




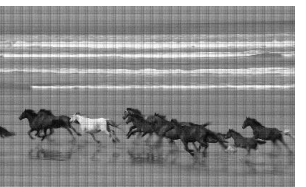









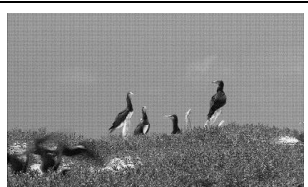

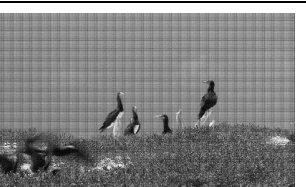

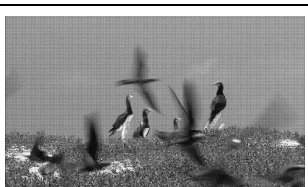

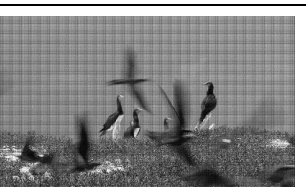



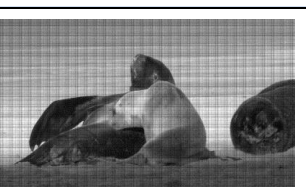
Image 1			
Original grayscale picture	Picture with image 1 encrypted with moments of Tchebichef and error RMES obtained	Picture with image 1 encrypted with moments of Krawtchouk and error RMES obtained	Picture with image 1 encrypted with moments of Charlier and error RMES obtained
 Frame 1	 Error: 0.008421582954157	 Error: 0.001842277213002	 Error: 0.019484637490130
 Frame 50	 Error: 0.008589163418294	 Error: 0.001532237233000	 Error: 0.01941656333445
 Frame 100	 Error: 0.008628113474130	 Error: 0.00159156502608	 Error: 0.019411536123924
 Frame 150	 Error: 0.009169532422789	 Error: 0.002070684641604	 Error: 0.02048594842581
 Frame 200	 Error: 0.009190412353122	 Error: 0.002054396309360	 Error: 0.02030570587382
 Frame 225	 Error: 0.008499093782543	 Error: 0.001538894832647	 Error: 0.019095206115332

Table 3. Comparison of some pictures of the original video and the three videos with the image 1 encrypted with each one of the families of the moments mentioned.


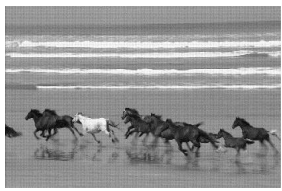

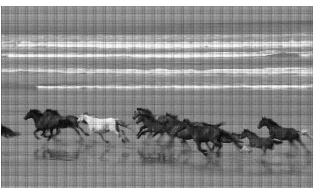











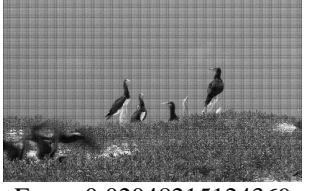

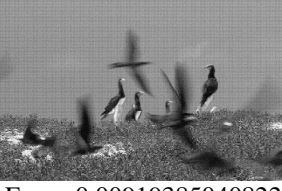

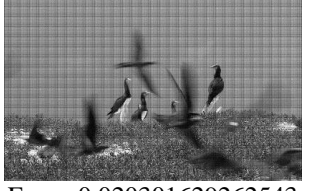




Image 2			
Original grayscale picture	Picture with image 2 encrypted with moments of Tchebichef and error RMES obtained	Picture with image 2 encrypted with moments of Krawtchouk and error RMES obtained	Picture with image 2 encrypted with moments of Charlier and error RMES obtained
 Frame 1	 Error:0.00842706855154	 Error: 0.001403586522355	 Error: 0.019487872709205
 Frame 50	 Error:0.00859207392774	 Error: 0.00153223642982	 Error: 0.01941783473805
 Frame 100	 Error:0.00862708224276	 Error: 0.001591565440147	 Error: 0.01941288515722
 Frame 150	 Error: 0.00917566466352	 Error: 0.002070686629763	 Error: 0.02048215124369
 Frame 200	 Error: 0.00919385040822	 Error: 0.002054401075617	 Error: 0.020301629262543
 Frame 225	 Error: 0.00850101513974	 Error: 0.001538896055511	 Error: 0.019094919814542

Table 4. Comparison of some pictures of the original video and the three videos with the image 2 encrypted with each one of the families of the moments mentioned.




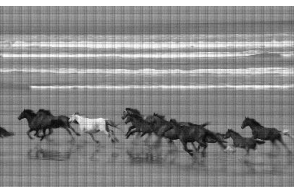









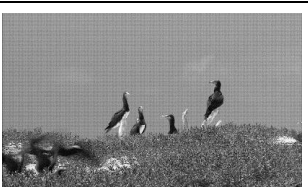

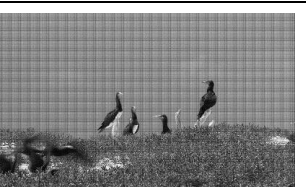

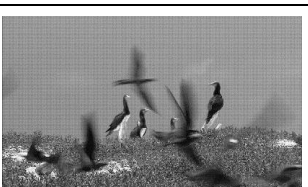

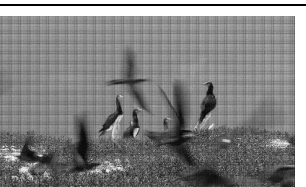



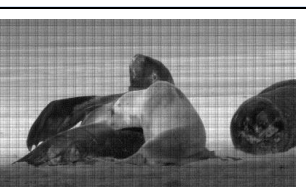
Image 3			
Original grayscale picture	Picture with image 3 encrypted with moments of Tchebichef and error RMES obtained	Picture with image 3 encrypted with moments of Krawtchouk and error RMES obtained	Picture with image 3 encrypted with moments of Charlier and error RMES obtained
 Frame 1	 Error: 0.00842299319818	 Error: 0.001403590220099	 Error: 0.01948373620824
 Frame 50	 Error: 0.008591555208954	 Error: 0.001532234654832	 Error: 0.01941815709640
 Frame 100	 Error: 0.008624582626406	 Error: 0.001591562178145	 Error: 0.01941308613414
 Frame 150	 Error: 0.009158690680587	 Error: 0.002070692429613	 Error: 0.02048011477177
 Frame 200	 Error: 0.00920009851331	 Error: 0.002054403964607	 Error: 0.02029798818268
 Frame 225	 Error: 0.008500387383468	 Error: 0.001538897508497	 Error: 0.01909633809163

Table 5. Comparison of some pictures of the original video and the three videos with the image 3 encrypted with each one of the families of the moments mentioned.

Next, the RMES graphics of the encryption of the three images in each frame of the video are shown in Fig.12.

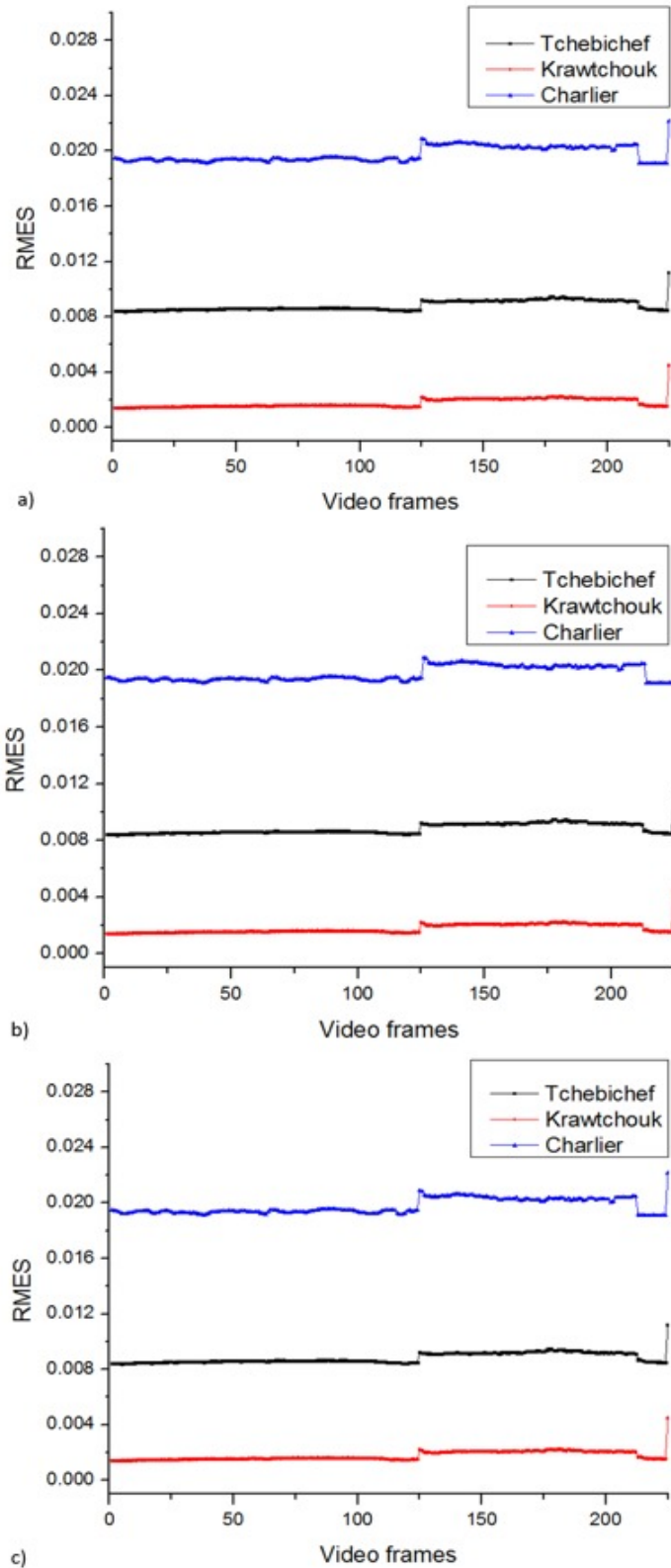


Figure 12. Graphs obtained from the RMES of encryption by video frame, a) Image 1, b) Image 2, c) Image 3.

On the other hand, the three test images were recovered from the three videos obtained as a result of the proposed algorithm, and the recovery error of each one was calculated using the RMES. The results are shown in Table 6.




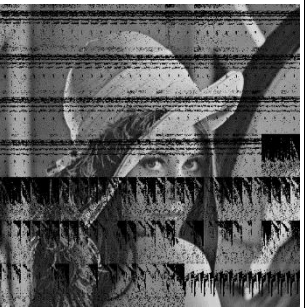
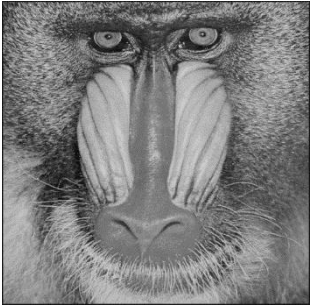
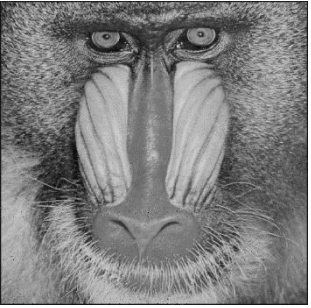
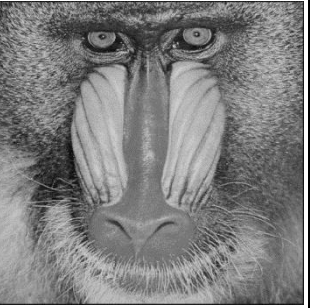
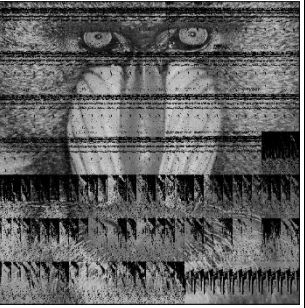
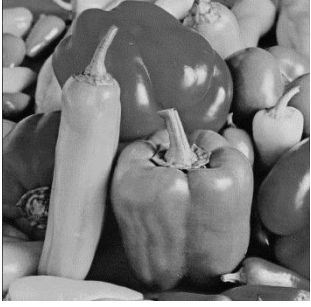
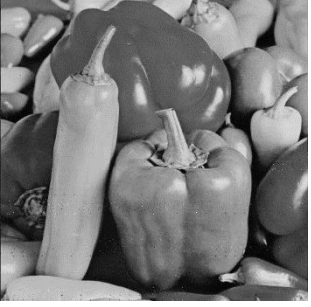
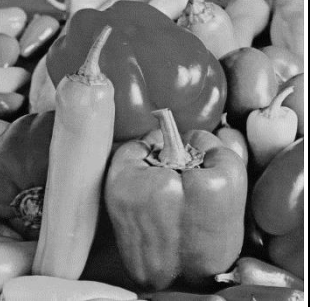
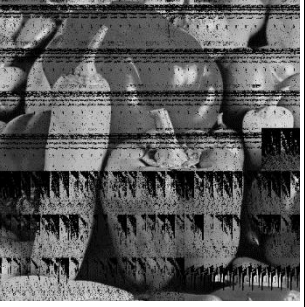
Original image	Image recovered by Tchebichef moments,	Image recovered by Krawtchouk moments	Image recovered by Charlier moments
 Image 1	 RMES:0.00080549	 RMES: 0	 RMES: 0.33816496594751
 Image 2	 RMES: 0.0008011398870	 RMES: 0	 RMES: 0.30919267910203
 Image 3	 RMES: 0.0007002511305	 RMES: 0	 RMES: 0.3306980051737

Table 6. Comparison of the original images and the recovered images with each of the families of moments mentioned.

5. CONCLUSIONS

According to the distribution of values for each family of orthogonal polynomials as shown in Fig. 1, it can be observed that the distribution of the Tchebichef polynomials is more uniform in comparison to Krawtchouk and Charlier polynomials. Therefore, better results would be expected with these polynomials. Once the results shown in section 4 were obtained, the comparison was performed using the RMES, in which it was observed that the Krawtchouk moments with p

= 0.5 perform better for encryption and decryption of each image. These moments allow for complete recovery of the images thanks to the characteristic form of the Krawtchouk polynomials. Encrypting an image in a sequence of images can enhance information security through the use of videos. Furthermore, this procedure can be used for watermarking the copyright in a video sequence.

In this case, for the process of encrypting an image of 512 x 512, a total of 225 of the 900 frames of the video were used for each family of moments, which is equivalent to 7.5 seconds of video, in this way It is possible to perform the encryption of larger images, as long as the video contains the number of frames required.

REFERENCES

1. B. Zitova and J. Flusser, "Image registration methods: a survey," *Image Vis. Comput.* 21(11), 977–1000 (2003).
2. S. Farokhi et al., "Rotation and noise invariant near-infrared face recognition by means of Zernike moments and spectral regression discriminant analysis," *J. Electron.* (2013).
3. C. Camacho-Bello and J. Baez-Rojas, "Angle estimation using Hahn moments for image analysis," *Lec. Notes Comput. Sci.* 8827, 127–134 (2014).
4. C. Singh and S. K. Ranade, "Rotation invariant moments and transforms for geometrically invariant image watermarking," *J. Electron. Imaging* 22(1), 013034 (2013).
5. A. Padilla-Vivanco et al., "Comparative analysis of pattern reconstruction using orthogonal moments," *Opt. Eng.* 46(1), 017002 (2007).
6. J. F. Mangin et al., "Brain morphometry using 3D moment invariants," *Med. Image Anal.* 8(3), 187–196 (2004).
7. E. Maalouf, B. Colicchio, and A. Dieterlen, "Fluorescence microscopythree-dimensional depth variant point spread function interpolation using Zernike moments," *J. Opt. Soc. Am. A* 28(9), 1864–1870 (2011).
8. G. Papakostas, "Moments and Moment Invariants: Theory and Applications," Science Gate Publishing, Xhanti, Greece (2014).
9. G. AlGarni and M. Hamiane, "A novel technique for automatic shoe print image retrieval," *Forensic Sci. Int.* 181(1), 10–14 (2008).
10. C. Camacho-Bello and J. Baez-Rojas, "Krawtchouk moments for gait phase detection," *Lec. Notes Comput. Sci.* 8827, 787–793 (2014).
11. César Camacho-Bello, Alfonso Padilla-Vivanco, Carina Toxqui-Quitl, José Javier Báez-Rojas, "Reconstruction of color biomedical images by means of quaternion generic Jacobi-Fourier moments in the framework of polar pixels," *J. Med. Imag.* 3(1), 014004 (2016).
12. Ali Mohammad Al-Haj," *Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications*",2010.
13. Luis M. Ledesma-Carrillo, Misael Lopez-Ramirez, Eduardo Cabal-Yepez, Jorge Ojeda-Castaneda, Carlos Rodriguez-Donate, Rocio A. Lizarraga-Morales," *FPGA-Based Reconfigurable Unit for Image Encryption Using Orthogonal Functions*", 978-1-5090-0079-1/16/\$31.00 ©2016 IEEE.
14. Shiraz Ahmad, Zhe-Ming Lu2, "Feature-based Watermarking using Discrete Orthogonal Hahn Moment Invariants",
15. G.A. Papakostas, E.D. Tsougenis and D.E. Koulouriotis," *Moment-based Local Image Watermarking via Genetic Optimization*", *Applied Mathematics and Computation*, vol. 227, pp. 222-236, 2014.
16. Nitin Singhal, Young-Yoon Lee, Chang-Su Kim, Sang-Uk Lee," *Robust image watermarking using local Zernike moments*",2009.
17. Sudhanshu Suhas Gongea, and Ashok Ghatolb," *Aggregation of Discrete Cosine Transform Digital Image Watermarking with Advanced Encryption Standard Technique*", *Procedia Computer Science* 89 (2016) 732 – 742.
18. Ingemar J. Cox, Senior Member, IEEE, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, Member, IEEE, *Secure Spread Spectrum Watermarking for Multimedia*.
19. G.A. Papakostas, E.D. Tsougenis and D.E. Koulouriotis," *Moment-based Local Image Watermarking via Genetic Optimization*", *Applied Mathematics and Computation*, vol. 227, pp. 222-236, 2014.
20. I.J.Cox.G., " *Digital Watermarking and Steganography*", Deorr,2006.
21. M. K. Hu, "Visual pattern recognition by moment invariants," *IRE Trans. Inf. Theory* 8(2), 179–187 (1962).
22. H. Zhu1 M. Liu2 H. Shu3 H. Zhang3 L. Luo3, "General form for obtaining discrete orthogonal moments", 2010