Noname manuscript No.
(will be inserted by the editor)

Fast chaotic encryption scheme based on separable moments and parallel computing

Abdelhalim Kamrani* · Khalid Zenkouar · Said Najah · Hakim El Fadili

Received: date / Accepted: date

Abstract In this paper, we propose three novel image encryption algorithms. Separable moments and parallel computing are combined in order to enhance the security aspect and time performance. The three proposed algorithms are based on TKM (Tchebichef-Krawtchouk moments), THM (Tchebichef-Hahn moments) and KHM (Krawtchouk-Hahn moments) respectively. A novel chaotic scheme is introduced, which allows for the encryption steps to run simultaneously. The proposed algorithms are tested under several criteria and the experimental results show a remarkable resilience against all well-known attacks. Furthermore, the novel parallel encryption scheme exhibits a drastic improvement in the time performance. The proposed algorithms are compared to the state-of-the-art methods and they stand out as a promising choice for reliable use in real world applications.

Keywords Image encryption · Separable moments · Chaos cryptography · Parallel computing

A. Kamrani (corresponding author)
Laboratory of Intelligent Systems and Application (LSIA), Faculty of Sciences and Technology, Sidi Mohamed Ben Abdellah University, Fez, Morocco
Phone: +1 781-666-7741
E-mail: abdelhalim.kamrani@usmba.ac.ma

K. Zenkouar
Laboratory of Intelligent Systems and Application (LSIA), Faculty of Sciences and Technology, Sidi Mohamed Ben Abdellah University, Fez, Morocco
E-mail: khalid.zenkouar@usmba.ac.ma

S. Najah
Laboratory of Intelligent Systems and Application (LSIA), Faculty of Sciences and Technology, Sidi Mohamed Ben Abdellah University, Fez, Morocco
E-mail: said.najah@usmba.ac.ma

H. El Fadili
Ecole Nationale des Sciences Appliquees of Fez, University Sidi Mohamed Ben Abdellah, Fez, Morocco
E-mail: hakim.elfadili@usmba.ac.ma

1 Introduction

Cyber security plays a huge role in today's world, as the networks expand the interconnection of the world's information systems, information security has become a matter of global interest and importance. Its goal is to ensure business continuity and minimize business damage by limiting the impact of security incidents [27]. In the ISO/IEC 27002 (2005) standard [28], information security is defined as the preservation of the Confidentiality, Integrity and Availability of information. The so called CIA triangle is the industry standard for the characteristics of information that needs to be protected [28]. The confidentiality issue can well be addressed using encryption [27]. Encryption protects the confidentiality of the data by transforming the information (plaintext) into unintelligible form (ciphertext) using mathematical algorithms and a secret information (key) [4]. So that if an unauthorized entity have access to the storage device or communication channel, it can not see the "hidden" data.

While encryption techniques can be used for any type of data, image encryption presents particular challenges compared to text encryption due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels. Thus, the traditional ciphers such as DES, IDEA and RSA are not suitable for practical image encryption, since they require a large computational time and high-computing resources [13] [39]. In recent years, different algorithms have been specifically designed for image encryption [38] [14] [37]. These algorithms can be classified into two categories: algorithms operating in space domain and algorithms operating in frequency domain [11] [17] [8] [7]. While the former tend to be a more "direct" approach, since they manipulate the image pixels directly, they come with a downside by causing un-correlation among pixels and thus making the cipher image uncompressible [10]. The latter algorithms instead of image pixels deal with the coefficients obtained in the transform domain, these algorithms were reported to have higher efficiency, they are more robust against image processing operations and can make lossless recovery of the original image [3] [16].

A common problem in image encryption domain is the "speed vs. security" dilemma [29]. While the recently proposed algorithms tend to be more and more secure, they come at a cost, which is computation speed [9][42]. In fact, chaos based algorithms –which are the predominant schemes in image encryption area- are generally a "two stages based process", namely, confusion and diffusion. These two separated stages are repeated until a satisfactory level of security is obtained [21]. The more these steps are repeated the more secure the algorithm is, and the slower it gets [21] [12]. Several works have been introduced in order to enhance the time performance of image encryption algorithms while keeping a required level of security [32] [23] [9] [33]. While these works present much enhancement toward resolving the dilemma mentioned above, they are not suitable for real world applications, because they either require some specific settings or are still limited in time performance for real world scenarios. Thus, our work aims to tackle the above-mentioned

problem by presenting a fast and secure encryption algorithm based on chaos and parallel computing. In this work, we have opted for using separable moments as the transform domain for encryption. This choice is motivated by the remarkable results shown in different areas of image processing [36] [2] [35]. In fact, the theory of moments have been introduced into the image encryption domain and showed remarkable results [6] [18] [15]. In [11] we made a first attempt to explore the use of the transform domain of moments for encryption. In this work, we used a logistic map to confuse and then diffuse the moments' coefficients obtained using: Tchebichef, Krawtchouk, Hahn, Dual Hahn and Racah moments. We argued that the moments' based encryption algorithms outperform state-of-the-art methods [11]. Recently, a new family of moments called separable moments [41] has been proposed, the image is represented as the tensor product of two different or same orthogonal polynomials in one variable. The authors have proposed new basis functions for two-dimensional orthogonal moments, as a product of well-known orthogonal moments. They claim that the SMs manage to adopt properties from both polynomials based on which are defined [41] [26]. A number of these proposed moments outperformed the original moments [26]. Since their introduction, different variants of separable moments were proposed dealing with different setups [2] [22] [36].

In this paper, we propose three novel encryption algorithms based on separable moments and chaos. We propose a novel scheme that allows several steps to run simultaneously. We add an new step in the encryption process called "blocks' permutation". Different threads perform the simultaneous steps by using parallel computing. As a result, the experimental results show that the computational cost is significantly enhanced while improving the security performance of the proposed algorithms. The three proposed algorithms are based on the same scheme; they differ by the separable moments function used. We investigate in particular the combinations: Tchebichef-Krawtchouk moments (TKM), Tchebichef-Hahn (THM) and Krawtchouk-Hahn moments (KHM), the choice of these particular moments is justified by the results presented in [11]. In fact, Tchebichef, Krawtchouk and Hahn moments were the most promising transformations in terms of security performance. Our contributions in this paper are summarized as follows:

- Improving the security aspect of the encryption algorithms by adding a new layer of security on top of the classical (confusion / diffusion) scheme, namely: block permutation.
- Proposing a scheme based on parallel computing that allows for several steps to run simultaneously which reduces the time cost of the proposed algorithms.
- Introducing SM moments into the domain of image encryption.

We have organized the rest of this paper in the following way: background on separable moments and chaos theory is given in section 2. Section 3 presents details about the proposed algorithms. The efficiency of the these algorithms is demonstrated in section 4 through experimental results. Finally a conclusion is drawn in section 5.

2 Relevant knowledge

Our aim is to make this paper as self-contained as possible. In this regard, the current section serves as a theoretical background for the concepts used in this article. We briefly discuss the theory of image moments and show how they are be computed then we present the logistic map and give some of its important properties.

2.1 Separable moments

Hu [6] first introduced image moments into image analysis in 1961, he proposed geometric moments for pattern recognition. These moments are not orthogonal, which causes redundancy of information. To overcome this drawback, Teague [25] proposed moments with orthogonal basis functions namely: Legendre and Zernike. While these moments allow for minimum information redundancy they have some disadvantages due to their continuity [19] [37] such as numerical approximation of continuous integrals, large variation in the dynamic range of values and coordinate space transformation. To eliminate these errors, the discrete orthogonal moments such as Tchebichef [19] Krawtchouk [37] and Hahn [40] have been introduced in image analysis. The basis functions' for these algorithms satisfy the orthogonality property, thus yield to a superior image representation. Indeed, it seems encouraging to produce new moments' families by combining separable discrete orthogonal polynomials [26].

Separable moments were recently introduced by Zhu [41], these moments are constructed by combining different continuous or discrete orthogonal polynomials. The SMs manage to adopt properties from both polynomials on which they are defined [41].The general formula to compute discrete orthogonal moments with order n and repetition m is as follows:

$$M_{nm} = NF \times \sum_{i=1}^{N} \sum_{j=1}^{N} kernel_{nm}(x_i, y_j) \times f(x_i, y_j) \tag{1}$$

Where $kernel_{nm}$ is the moments kernel that consists of specific polynomials of order n and repetition m and it constitutes the orthogonal basis. $f(x, y)$ is the original image of size $N \times N$ and NF is the normalization factor. The coefficients of each moments' family can be computed using the corresponding kernel and NF.

The original image can be reconstructed from the moments' coefficients using the formula:

$$F(x_i, y_j) = \sum_{n=1}^{N} \sum_{m=1}^{N} kernel_{nm}(x_i, y_j) \times M_{nm} \tag{2}$$

The properties of the separable moments used in this paper are summarized in the table 1.

Table 1

Moments'	Kernel form	Polynomial form
TKM	$t_n(x) \times K_m(y;p_2,N)$	$t_n(x) = (1-N)_n {}_3F_2(-n,-x,1+n;1,1-N;1)$, $K_m(x;p,N) = \sum_{k=0}^{N} a_{k,m,p}x^k$
THM	$t_n(x) \times h_m^{\mu,\nu}(x,N)$	$t_n(x) = (1-N)_n {}_3F_2(-n,-x,1+n;1,1-N;1)$, $h_m^{(u,v)}(x,N) = (N+\nu-1)_m(N-1)_m$ $\times \sum_{k=0}^{m}(-1)^k \frac{(-m)_k(-x)_k(2N+\mu+\nu-m-1)_k}{(N+\nu-1)_k(N-1)_k}\frac{1}{k!}$
KHM	$K_n(y;p_2,N) \times h_m^{\mu,\nu}(x,N)$	$K_n(x;p,N) = \sum_{k=0}^{N} a_{k,n,p}x^k, h_m^{(u,v)}(x,N) = (N+\nu-1)_m(N-1)_m$ $\times \sum_{k=0}^{m}(-1)^k \frac{(-m)_k(-x)_k(2N+\mu+\nu-m-1)_k}{(N+\nu-1)_k(N-1)_k}\frac{1}{k!}$

2.2 Logistic map

Chaos encryption systems are extensively used in the field of image encryption due to their ergodicity, sensitive dependence on initial conditions and control parameters. The classical scheme for chaos based encryption algorithms is depicted in figure 1. The encryption algorithm comprises of two main steps, i.e. confusion and diffusion. In the confusion step the pixels are permuted according to a pseudo-random chaotic map , this step spreads the information in the image which loosens the dependence between the image pixels. In the diffusion step, the pixels' values are altered making the image unrecognizable. Logistic maps are the most used chaotic maps for generation random sequences in chaos based encryption algorithms due to their low complexity, which makes them suitable to design fast architecture of image encryption [34]. The logistic map is defined as,

$$x_{n+1} = \mu x_n(1-x_n) \quad x_n \epsilon (0,4] \tag{3}$$

x_n is the state variable, n the number of iterations and μ is a parameter in the range of parameter (0, 4]. The bifurcation diagram of the logistic map is depicted in the graph 2.

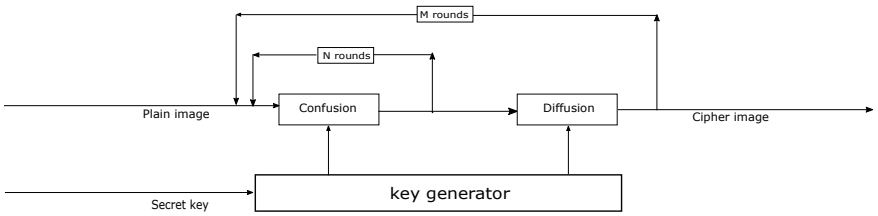

Fig. 1 General scheme for chaos based encryption

When μ is around 3.57, the logistic map exhibits a chaotic behavior. In this region, slight variations in the initial conditions lead to highly different results.

In this paper, we set the parameter $\mu = 3.999$ having positive Lyapunov exponents as shown in Figure 3

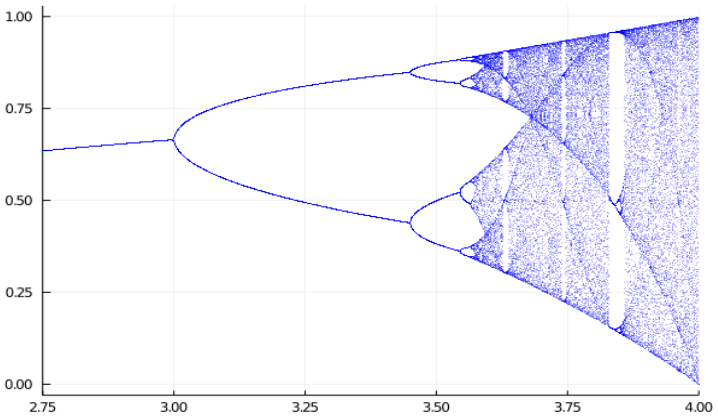

Fig. 2 Bifurcation diagram for the logistic map

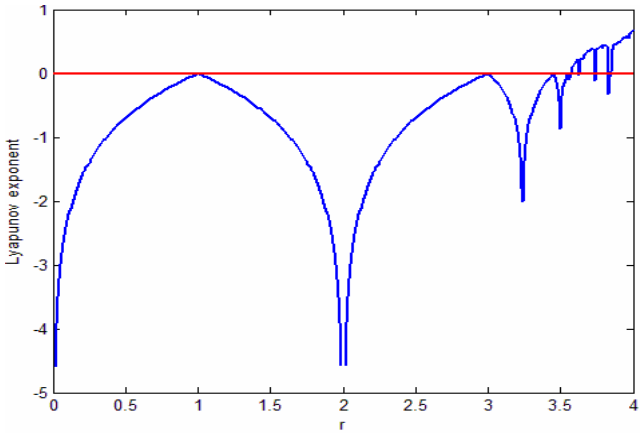

Fig. 3 Lyapunov exponent with $\mu = 3.999$

3 The proposed encryption algorithms

In this section we present a step-by-step overview of the proposed algorithms. Three algorithms are proposed which differ by the moments functions used as the transform domain. Without loss of generality, an attempt to explore the use of separable moments as the transform domain for encryption was made. The authors investigated in particular the combinations: TKM, THM, KHM, the choice of these particular moments is justified by the results presented in [11]. In fact Tchebichef, Krawtchouk and Hahn moments were the most promising ones in terms of security performance.

The proposed scheme allows for reduced computational time without harming the security performance. In fact, where compared to classical encryption schemes [11] [20] [5], an additional layer of security was added, namely blocks' permutation. Furthermore, one of our main contributions in this paper is

proposing an encryption scheme with steps that are performed simultaneously. Thus, parallel computing is used for implementing the proposed algorithms. In this regard, representing the image in transform domain of moments and the blocks' permutation are done simultaneously and they are run by two different threads. Moreover the pixels' confusion and diffusion steps are done separately involving two other threads. The detailed implementations of the proposed algorithms is described below.

3.1 Encryption

The general encryption scheme used in the proposed algorithms is depicted in Fig 4. The encryption process is divided into two main steps, namely "moments' computation / block permutation" and "confusion / diffusion". Each step is composed of two sub-steps that are performed separately and thus run by different threads.

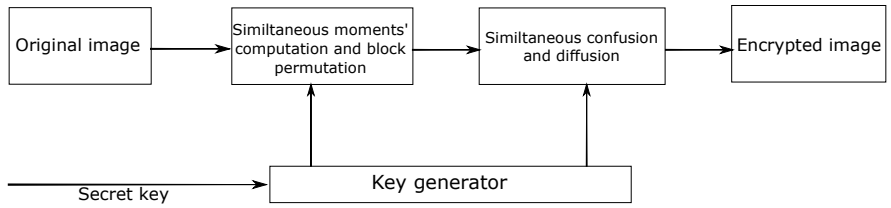

Fig. 4 The proposed encryption scheme

step 1) Key generation: We use an external key K of length 192 bits, the key is divided into 3 segments: K_1, K_2 and K_3. These segments are used as the initial conditions for the logistic maps involved in the encryption process. Logistic maps take an initial value between 0 and 1, so in order to adapt the segments K_1, K_2 and K_3 as initial conditions we perform the following mathematical operations:

We note each segment K_i in its binary form: $K_1 = K_{11}, K_{12} \dots K_{164}$. $K_2 = K_{21}, K_{22} \dots K_{264}$. $K_3 = K_{31}, K_{32} \dots K_{364}$. Then the initial values for the logistic maps are computed as follows:

$X_0 = (K_{11} \times 2^0 + K_{12} \times 2^1 + \dots + K_{164} \times 2^{63})/2^{64}$

$Y_0 = (K_{21} \times 2^0 + K_{22} \times 2^1 + \dots + K_{264} \times 2^{63})/2^{64}$

$Z_0 = (K_{31} \times 2^0 + K_{32} \times 2^1 + \dots + K_{364} \times 2^{63})/2^{64}$

Where X_0, Y_0 and Z_0 are the initial values for the logistic maps X, Y and Z respectively.

step 2) Generating random sequences:

Three logistic maps are used, X, Y and Z to generate random sequences. The generated sequences are used for block permutation, pixels' permutation and pixels' diffusion respectively.

1. Using logistic map X and initial value X_0, generate a random sequence L of size l ($l = [M \times N \times 5]/64$ experiment based). In order to make the L suitable for block permutation we do the following operations:
   (a) $L'_i = [L_i \times 10^{14}] mod(NB)$, where NB = Number of the 8×8 blocks in the image, i.e. $M \times N/64$.
   (b) Delete all duplicates from L'.
   (c) Shrink the size of L' to NB.
2. Using logistic map Y and initial value Y_0, generate a random sequence T of size t ($t = M \times N \times 3$ experiment based).
   (a) $T'_i = [T_i \times 10^{14}] mod(M \times N)$, where M and N are the dimensions of the input image.
   (b) Delete duplicates from T'.
   (c) Shrink size of T' to $M \times N$.
3. Using logistic map Z and initial value Z_0, generate random sequence S of size $s = M \times N$.

Step 3) Block permutation and moments' computation:

Input: image I of size $M \times N$, L (random sequence generated in step 2).
Output: B matrix of size $M \times N$.

- Adjust the image size if the total number of pixels is not a multiple of 64.
- Partition the image into P blocks of size 8×8.
- For each block i:

Thread 1: compute moments' coefficients using the corresponding separable moments namely, TKM (Tchebichef Krawtchouk moments), THM (Tchebichef Hahn moments) and HKM (Hahn Krawtchouk moments).

Thread 2: change block position to L_i.

- Store the block at the position L_i in the matrix B.

Step 4) Confusion / diffusion process:

Input: matrix B, S and T (random sequences generated in step 2).
Output: E encrypted image.

- Convert the image into an array A of size $M \times N$.
- For each pixel j:

Thread 1: diffusion, change pixel's value according to $A_j \; XOR \; T_j$.
Thread 2: confusion: Change pixel's position to S_j.

- Store calculated value at position S_j in matrix E.

3.2 Decryption:

Decryption is the reverse procedure of encryption which - given the appropriate key- it allows to recover the original image from the encrypted one. The decryption procedure is similar to the encryption process except that some steps are in reversed order.

Steps 1 and 2: The same encryption key generated in the step 1 and the random sequences generated in the step 2 of the encryption algorithms are used for the decryption process.

Step 3: Reverse confusion diffusion process.

Input: E encrypted image, S and T (random sequences generated in step 2).

Output: Matrix F.

- The image is transformed to an array of size $M \times N$ notated W.

Thread 1: change pixel value according to $W_i \ XOR \ T_i$.

Thread 2: change pixel position according to S_i.

- Reverse the computed array to a matrix F of size $M \times N$.

Step 4: Reverse blocks' permutation and inverse moments' computation.

Input: matrix F, L (random sequence generated in step 2).

Output: D decrypted image.

Divide the image into blocks of size 8×8 and for each block j:

Thread 1: compute inverse moments.

Thread 2: change block position according to L.

- Store the computed blocks into D.

The decryption scheme is summarized in fig 5:

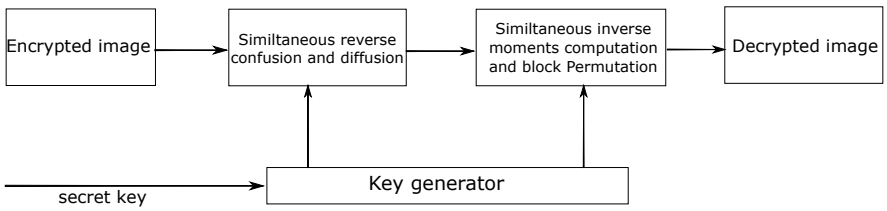

Fig. 5 The decryption scheme

4 Experimental study

In this section, we validate the performance of the proposed algorithms by running several tests. We use five grey-scale well-known images: "Lena", "Baboon", "Cameraman", "Boats", and "Livingroom" of size 512×512. Then the results are compared with state-of-the-art algorithms in [31] [30] [24] [11]. All algorithms are implemented using MATLAB 11 on a laptop with an Intel Core i7, 2.7 GHz CPU, 8 gigabyte memory and 256 gigabyte hard disk operating on Windows 10. The analyses of security and performance are given below.

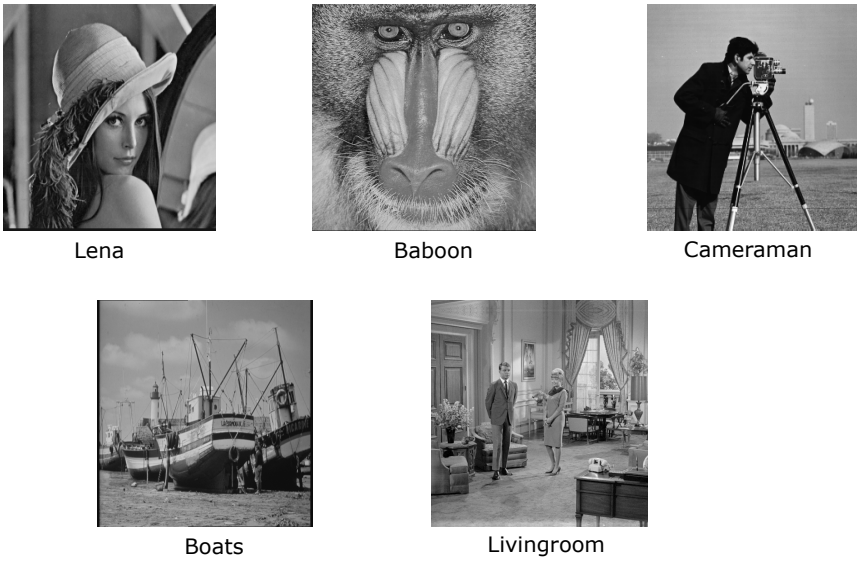

Fig. 6 Images used for the experiments

4.1 Key space analysis

A secure encryption scheme should be sensitive to the cipher key, the key space should be large enough to make brute-force attack infeasible. The key space of the proposed algorithms is large enough to make it secure against brute-force attack. The total key space is 2^{192} which is secure since the key space is larger than 2^{100} [1].

4.2 Differential attacks

To resist differential attacks, the encryption algorithm should exhibit a great image sensitivity. By changing a pixel value of the plaintext image the encrypted image shows a qualitative transformation. The differential attacks criteria provides a security proof for chosen plaintext attacks. Two quantitative descriptors are used to demonstrate resistance against differential attacks, namely UACI (Unified Average Changing Intensity) and NPCR (Number of pixel change rate) defined by equations 6 and 4 respectively:

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100 \tag{4}$$

Table 2 NPCR results for the proposed algorithms compared to the state-of-the-art algorithms

NPCR	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [11]	Krawtchouk [11]	Hahn [11]	Ref [31]	Ref [30]	Ref [24]
Lena	99,8572	99,8321	99,8425	99,791	99,7559	99,7879	99,9961	99,9961	99,9955
Baboon	99,8944	99,798	99,8536	99,7955	99,8337	99,855	99,9953	99,996	99,9958
Cameraman	99,8234	99,8764	99,8896	99,7574	99,7437	99,8276	99,9959	99,996	99,9956
Boats	99,8247	99,8636	99,9005	99,7589	99,7681	99,8337	99,9955	99,9957	99,996
livingroom	99,7928	99,7779	99,7878	99,8093	99,7467	99,8276	99,9955	99,9954	99,9957

Table 3 UACI results for the proposed algorithms compared to the state-of-the-art algorithms

UACI	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [11]	Krawtchouk [11]	Hahn [11]	Ref [31]	Ref [30]	Ref [24]
Lena	33,47	33,327	33,551	29,158	32,249	28,659	33,232	33,198	33,174
Baboon	33,462	33,541	33,35	30,44	31,773	26,813	33,161	33,166	33,255
Cameraman	33,438	33,344	33,417	26,301	29,435	27,54	33,332	33,212	33,26
Boats	33,342	33,363	33,512	25,102	27,503	25,609	33,347	33,145	33,172
livingroom	33,505	33,449	33,325	28,157	30,979	26,703	33,312	33,267	33,26

Where W and H are the image width and height. $D(i,j)$ is defined as,

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{5}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right] \times 100 \tag{6}$$

When the $NPCR$ is around 99.6 and $UACI$ reaches approximately 33.4, the encryption is secure against differential attacks [29] [24].

We encrypt the test images listed in table 6 using the proposed encryption algorithm. We change one pixel value in the plain image and encrypt it again using the same algorithms. Results are shown in the tables 2 and 3 in contrast with state-of-the-art algorithms:

From tables 2 and 3 we see that all the algorithms are producing results near to the optimal values. Moreover, the proposed algorithms have demonstrated better results in terms of UACI and NPCR compared to state-of-the-art algorithms, which makes them more secure against differential attacks.

4.3 Statistical analysis

4.3.1 Histogram analysis

The histogram analysis implies counting the frequency distributions of image pixels. For an encrypted image the more evenly distributed the pixels values are the better the encryption algorithm is [24]. A good cryptosystem should hide the statistical properties of the encrypted image, in a histogram this is translated by a uniform distribution of the pixels' values. We encrypt the test

image 'Lena' with the three proposed encryption algorithms and then we plot the histograms of the encrypted images along with the original image. It can be clearly seen from the figure 7 that the histograms of the encrypted image are almost flat which makes these algorithms secure against statistical analysis.

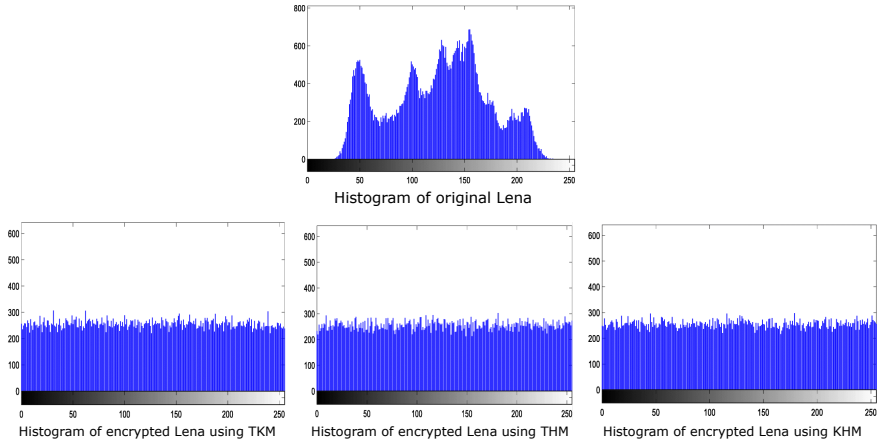

Fig. 7 Histogram analysis for the proposed encryption algorithms

4.3.2 Correlation of adjacent pixels

The correlation coefficient in image encryption is a statistical technique that measures the similarity between two images, e.g. the plain image and the cipher image. The correlation coefficient is used to evaluate the quality of a cryptosystem; it takes a value between -1 and 1. Zero correlation indicates an absence of correlation between the two images while a value of 1 means that the plain image and the cipher one are in perfect correlation. The smaller the absolute value of the correlation coefficient is, the more secure the encryption algorithm is. The correlation coefficient C.C is computed using the following formula:

$$C.C = \frac{Cov(x,y)}{\sigma_x \times \sigma_y} \tag{7}$$

$$\sigma_x = \sqrt{VAR(x)} \tag{8}$$

$$\sigma_y = \sqrt{VAR(y)} \tag{9}$$

$$VAR(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{10}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{11}$$

Table 4 Correlation coefficient for the proposed encryption algorithms compared to state-of-the-art algorithms

C.C	Plain image	P.TKM	P.THM	P.KHM	Tchebichef [11]	Krawtchouk [11]	Hahn [11]	Ref [31]	Ref [30]	Ref [24]
Horizontal	0,8263	0,00105	-0,0006	-0,003	0,0032	-0,088	0,0405	-0.0025	-0,088	0,0039
Vertical	0,9273	-0,0003	0,0007	0,0005	0,047	-0,00116	-0,0083	0.00126	0,079	0,002
Diagonal	0,867	0,001	-0,0005	0,0006	0,0088	0,021	-0,009	-0.006	0,096	0,076

Where x and y are pixels' positions of plain-text image and cipher-text image respectively, $Cov(x, y)$ is covariance, $VAR(x)$ is variance at pixel position x, σ_x is standard deviation and N is the total number of pixels.

We compute the correlation coefficient between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels for the Lena image. The results are depicted in table 4.

As illustrated in results' table, the correlation coefficients are near 0 for all the algorithms. Meanwhile, the newly proposed algorithms stand out from the other methods by showing results that are closer to 0. Hence the proposed algorithms are more robust against statistical attacks.

4.4 Information entropy analysis

Information entropy is a measure that describes quantitatively the pixels distribution in an image. It reflects the randomness and unpredictability of information. The entropy $H(m)$ of a message m can be measured by the formula 12:

$$H(m) = \sum_{i=0}^{M-1} p(m_i) log \frac{1}{m_i} \tag{12}$$

Where $p(m_i)$ represents the occurrence probability of a symbol m_i , M is the total number of symbols and log denotes base 2 logarithm. Therefore, the maximum value of H is 8, and the larger H is, the less likely there is an information leak. Table below lists comparison of information entropy of the proposed algorithms and state-of-the-art methods [11] [31] [30] [24]. All information entropy depicted in table **??** are close to 8, meaning that the cipher-images are close to a random source. Furthermore, one can clearly see that the proposed algorithms outperforms state-of-the-art methods.

4.5 Speed analysis

One of our main contributions in this paper is proposing a secure encryption scheme that is suitable for parallel computing. By allowing the encryption steps to run simultaneously, we are able to reduce drastically the time complexity without compromising the security performance of the proposed algorithms.

Table 5 Entropy results for the proposed algorithms compared to the state-of-the-art algorithms

Entropy	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [11]	Krawtchouk [11]	Hahn [11]	Ref [31]	Ref [30]	Ref [24]
Lena	7,9982	7,9985	7,9997	7,9946	7,9953	7,9955	7,9964	7,9967	7,996
Baboon	7,9982	7,9989	7,9995	7,995	7,9956	7,9956	7,9959	7,9963	7,9961
Cameraman	7,9978	7,9992	7,9985	7,9944	7,9953	7,9955	7,9961	7,996	7,9952
Boats	7,9984	7,9981	7,9978	7,9946	7,9954	7,9956	7,9966	7,9966	7,9953
livingroom	7,9986	7,9983	7,9983	7,9945	7,9953	7,9956	7,9961	7,9955	7,9966

Table 6 Speed analysis for the proposed algorithms compared to the state-of-the-art algorithms

Image size	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [11]	Krawtchouk [11]	Hahn [11]	Ref [31]	Ref [30]	Ref [24]
128*128	0,0112	0,0126	0,0114	0,1148	0,0725	0,1747	0,0355	0,0263	0,0774
256*256	0,0164	0,0243	0,0223	0,285	0,4422	0,3713	0,46	0,442	0,11794
512*512	0,022	0,0333	0,0319	0,3949	0,7683	0,6207	0,979	0,466	0,27444
1024*1024	0,0493	0,0434	0,0479	0,8859	0,8671	0,7683	1,1361	0,975	0,78902

In order to further demonstrate the validity of the proposed algorithms, we analyze their time complexity for different image sizes, i.e. 128×128, 256×256, 512×512 and 1024×1024. The results are depicted in table 6, the unit time is seconds:

As it can be seen in the table 6. The proposed algorithms show an important improvement in the time complexity compared to state-of-the-art algorithms. The running time of the proposed algorithms is very short; these algorithms are very fast and have good applicability.

In this section we have presented the experimental results run on the proposed algorithms, key space analysis, differential and statistical attacks, information entropy and speed analysis were means to validate these newly proposed algorithms. We came to the conclusion that these algorithms are robust against all types of known attacks and we've witnessed their superiority to the state-of-the art methods.

5 Conclusion

In this paper, we introduced three novel encryption algorithms based on separable moments and parallel computing. Three families of separable moments were employed as the transfer domain for the encryption namely, TKM (Tchebichef-Krawtchouk moments), THM (Tchebichef-Hahn moments) and KHM (Krawtchouk-Hahn moments). A new layer of security was added on top of the traditional chaotic encryption scheme. A new scheme based on parallel computation was introduced which allows for different steps to run simultaneously.
The experimental study showed the effectiveness of the newly introduced encryption algorithms. According to the presented results, we conclude that the proposed algorithms are secure against all types of known attacks and are

fast enough to be implemented in real world application. A comparative study witch state-of-the-art methods was performed where we showed the superiority of the newly proposed algorithms.

As a conclusion, given presented results of these new algorithms, we are confident about their ability to be used in real world scenarios. Thus we will focus on our future works on implementing these algorithms in real-time video encryption.

Acknowledgements The authors thankfully acknowledge the Laboratory of Intelligent Systems and Applications (LSIA) for his support to achieve this work.

Statements and Declarations

The authors declare no conflict of interest.
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare no conflict of interest.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data availability

All data generated or analyzed during this study are included in this published article

References

1. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos **16**(08), 2129–2151 (2006)
2. Batioua, I., Benouini, R., Zenkouar, K., Zahi, A., et al.: 3d image analysis by separable discrete orthogonal moments based on krawtchouk and tchebichef polynomials. Pattern Recognition **71**, 264–277 (2017)
3. Guan, M., Yang, X., Hu, W.: Chaotic image encryption algorithm using frequency-domain dna encoding. IET image processing **13**(9), 1535–1539 (2019)
4. Hankerson, D., Hoffman, G., Leonard, D.A., Lindner, C.C., Phelps, K.T., Rodger, C.A., Wall, J.R.: Coding theory and cryptography: the essentials. CRC Press (2000)
5. Hu, G., Li, B.: A uniform chaotic system with extended parameter range for image encryption. Nonlinear Dynamics **103**(3), 2819–2840 (2021)

6. Hu, M.K.: Visual pattern recognition by moment invariants. IRE transactions on information theory **8**(2), 179–187 (1962)
7. Hua, Z., Jin, F., Xu, B., Huang, H.: 2d logistic-sine-coupling map for image encryption. Signal Processing **149**, 148–161 (2018)
8. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Information Sciences **480**, 403–419 (2019)
9. Janakiraman, S., Thenmozhi, K., Rayappan, J.B.B., Amirtharajan, R.: Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller. Microprocessors and Microsystems **56**, 1–12 (2018)
10. Jiang, N.Z.X., Lan, X.: Advances in machine vision, image processing, and pattern analysis. In: International Workshop on Intelligent Computing in Pattern Analysis/Synthesis, IWICPAS. Springer (2006)
11. Kamrani, A., Zenkouar, K., Najah, S.: A new set of image encryption algorithms based on discrete orthogonal moments and chaos theory. Multimedia Tools and Applications **79**(27), 20263–20279 (2020)
12. Khedr, W.I.: A new efficient and configurable image encryption structure for secure transmission. Multimedia Tools and Applications pp. 1–25 (2019)
13. Li, S., Chen, G., Cheung, A., Bhargava, B., Lo, K.T.: On the design of perceptual mpeg-video encryption algorithms. IEEE Transactions on Circuits and Systems for Video Technology **17**(2), 214–223 (2007)
14. Li, S., Li, C., Chen, G., Zhang, D., Bourbakis, N.G.: A general cryptanalysis of permutation-only multimedia encryption algorithms. IACR's Cryptology ePrint Archive: Report **374**, 2004 (2004)
15. Lin, H., Si, J., Abousleman, G.P.: Orthogonal rotation-invariant moments for digital image processing. IEEE transactions on image processing **17**(3), 272–282 (2008)
16. Liu, S., Guo, C., Sheridan, J.T.: A review of optical image encryption techniques. Optics & Laser Technology **57**, 327–342 (2014)
17. Lu, Q., Zhu, C., Deng, X.: An efficient image encryption scheme based on the lss chaotic map and single s-box. IEEE Access **8**, 25664–25678 (2020)
18. Markandey, V., deFigueiredo, R.: Robot sensing techniques based on high-dimensional moment invariants and tensors. IEEE transactions on robotics and automation **8**(2), 186–195 (1992)
19. Mukundan, R., Ong, S., Lee, P.A.: Image analysis by tchebichef moments. IEEE Transactions on image Processing **10**(9), 1357–1364 (2001)
20. Ravichandran, D., Murthy, B., Balasubramanian, V., Fathima, S., Amirtharajan, R., et al.: An efficient medical image encryption using hybrid dna computing and chaos in transform domain. Medical & Biological Engineering & Computing **59**(3), 589–605 (2021)
21. Sankpal, P.R., Vijaya, P.: Image encryption using chaotic maps: a survey. In: 2014 fifth international conference on signal and image processing, pp. 102–107. IEEE (2014)
22. Sayyouri, M., Hmimid, A., Qjidaa, H.: Image analysis using separable discrete moments of charlier-hahn. Multimedia tools and applications **75**(1), 547–571 (2016)
23. Shah, A.A., Parah, S.A., Rashid, M., Elhoseny, M.: Efficient image encryption scheme based on generalized logistic map for real time image processing. Journal of Real-Time Image Processing **17**(6), 2139–2151 (2020)
24. Song, W., Zheng, Y., Fu, C., Shan, P.: A novel batch image encryption algorithm using parallel computing. Information Sciences **518**, 211–224 (2020)
25. Teague, M.R.: Image analysis via the general theory of moments. Josa **70**(8), 920–930 (1980)
26. Tsougenis, E., Papakostas, G.A., Koulouriotis, D.E.: Image watermarking via separable moments. multimedia tools and applications **74**(11), 3985–4012 (2015)
27. Von Solms, R.: Information security management (3): the code of practice for information security management (bs 7799). Information Management & Computer Security (1998)
28. Von Solms, R., Van Niekerk, J.: From information security to cyber security. computers & security **38**, 97–102 (2013)
29. Wang, X., Feng, L., Zhao, H.: Fast image encryption algorithm based on parallel computing system. Information Sciences **486**, 340–358 (2019)

30. Wang, X., Gao, S.: Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. Information sciences **507**, 16–36 (2020)
31. Wang, Y., Wong, K.W., Liao, X., Chen, G.: A new chaos-based fast image encryption algorithm. Applied soft computing **11**(1), 514–522 (2011)
32. Wong, K.W., Kwok, B.S.H., Law, W.S.: A fast image encryption scheme based on chaotic standard map. Physics Letters A **372**(15), 2645–2652 (2008)
33. Wu, G.C., Deng, Z.G., Baleanu, D., Zeng, D.Q.: New variable-order fractional chaotic systems for fast image encryption. Chaos: An Interdisciplinary Journal of Nonlinear Science **29**(8), 083103 (2019)
34. Xiang, H., Liu, L.: An improved digital logistic map and its application in image encryption. Multimedia Tools and Applications **79**(41), 30329–30355 (2020)
35. Xiao, B., Luo, J., Bi, X., Li, W., Chen, B.: Fractional discrete tchebyshev moments and their applications in image encryption and watermarking. Information Sciences **516**, 545–559 (2020)
36. Yamni, M., Karmouni, H., Sayyouri, M., Qjidaa, H.: Image watermarking using separable fractional moments of charlier–meixner. Journal of the Franklin Institute **358**(4), 2535–2560 (2021)
37. Yap, P.T., Paramesran, R., Ong, S.H.: Image analysis by krawtchouk moments. IEEE Transactions on image processing **12**(11), 1367–1377 (2003)
38. Ye, G., Pan, C., Huang, X., Mei, Q.: An efficient pixel-level chaotic image encryption algorithm. Nonlinear Dynamics **94**(1), 745–756 (2018)
39. Zhang, G., Liu, Q.: A novel image encryption method based on total shuffling scheme. Optics communications **284**(12), 2775–2780 (2011)
40. Zhou, J., Shu, H., Zhu, H., Toumoulin, C., Luo, L.: Image analysis by discrete orthogonal hahn moments. In: International Conference Image Analysis and Recognition, pp. 524–531. Springer (2005)
41. Zhu, H.: Image representation using separable two-dimensional continuous and discrete orthogonal moments. Pattern Recognition **45**(4), 1540–1558 (2012)
42. Zhu, S., Wang, G., Zhu, C.: A secure and fast image encryption scheme based on double chaotic s-boxes. Entropy **21**(8), 790 (2019)