Multimedia Tools and Applications (2020) 79:20263–20279
https://doi.org/10.1007/s11042-020-08879-6

A new set of image encryption algorithms based on discrete orthogonal moments and Chaos theory

Abdelhalim Kamrani[1] · Khalid Zenkouar[1] · Said Najah[1]

Received: 28 December 2018 / Revised: 11 March 2020 / Accepted: 23 March 2020 /
Published online: 16 April 2020

Abstract
In this paper, we introduce a new set of image encryption algorithms based on orthogonal discrete moments and chaos. Two logisitic maps are used to confuse and diffuse the moments' coefficients obtained using: Tchebichef, Krawtchouk, Hahn, dual Hahn and Racah. An external key of 128 bits is used as the encryption key, some mathematical operations are performed on the key to adapt it as the initial conditions of the logisitic maps. Several experiments are carried out to evaluate the security of the newly introduced algorithms: entropy, key space analysis, statistical and differential attacks. The results obtained show clearly that the proposed algorithms are secure enough to resist any type of known attacks. A comparative study with a similar algorithm operating in the Discrete Transform Domain (DCT) and the state-of-the-art methods validates the superiority of moments' domains particularly in highly textured images.

Keywords Image encryption · Discrete orthogonal moments · Chaos cryptography · DCT

1 Introduction

Encryption is the process of transforming "meaningful" data into unintelligible form. Its goal is reliable security in storage and secure transmission of content over the network [48]. Image encryption raises different challenges compared to text encryption. In fact, the digital images have certain characteristics such as: redundancy of data, strong correlation among adjacent pixels and the important size of the data. Thus, the traditional ciphers like IDEA, AES, DES, RSA etc. are not suitable for real time image encryption, since they require

✉ Abdelhalim Kamrani
abdelhalim.kamrani@usmba.ac.ma

Khalid Zenkouar
khalid.zenkouar@usmba.ac.ma

Said Najah
said.najah@usmba.ac.ma

[1] Laboratory of Intelligent Systems and Application (LSIA), Faculty of Sciences and Technology, Sidi Mohamed Ben Abdellah University, Fez, Morocco

a large computational time and high-computing resources [37, 74]. Different algorithms have been specifically designed for image encryption: Chaos [21, 30, 36, 69, 70, 72, 73], SCAN [12], S-Box [27], permutation only algorithms [38]. Among the proposed algorithms chaos was the most studied and has proved encouraging results [19, 65], due to its specific characteristics such as: pseudo randomness, ergodicity, high sensitivity to initial conditions and parameters [33, 63, 64].

In the last decade, a number of methods has been proposed in the literature for image encryption. Generally, image encryption methods can be classified in two categories: encryption algorithms using the space domain and other algorithms using the transform domain. The first category tends to be a direct approach since the image pixels are manipulated directly; however, it causes un-correlation among pixels, which makes the cipher image incompressible [28]. Conversely, the encryption methods based on the transform domains use, instead of image pixels, the coefficients obtained via the transform domain. These algorithms seem to have a higher efficiency, tend to be more robust against some image processing operations and can make a lossless recovery of the original image [23, 34, 35, 41, 58]. In the literature different transform domains had been used: J. Wu et al. [66] proposed an image encryption algorithm based on a reality-preserving Fractional Discrete Cosine Transform and a chaos-based generating sequence, which inherits the reality as well as non-periodicity of the Discrete Cosine Transform (DCT) matrix; furthermore, Generating Sequence (GS), which results from the multiplicity of FrDCT matrix root, is introduced to be an extra cipher key. Y. Luo et al. [42] introduced a symmetrical image encryption scheme in wavelet and time domain using Integer Wavelet Transform (IWT); the approximation coefficients are diffused by secret keys generated from a spatiotemporal chaotic system followed by inverse IWT to construct the diffused image. An image encryption algorithm based on spatiotemporal chaos in DCT domain was studied by G. Xin et al. [68] where every block is first permuted by placing the value on the same position of a chosen block using logistic map, then the signs of the permuted blocks are extracted and encrypted by the spatiotemporal chaos.

Note that, the most of these encryption methods make use of frequency domains as the transform domain. Meanwhile, image moments stand out as one of the most attractive transformations in image processing, they are better in terms of image description and are more robust to noise [6–8, 62]. In the recent past, different orthogonal polynomials have been studied. Continuous orthogonal moments have been first established [57], they are formed from basis functions of continuous orthogonal polynomials, and established remarkable capability in feature representation [31, 61]. However, while implementing these moments, several problems are encountered such as: numerical approximation of continuous integrals, large variation in the dynamic range of values and coordinate space transformation [45, 71]. These problems have motivated the researchers to look for discrete orthogonal moments as the basis set, thus no numerical approximation is involved which yields to a superior image reconstruction. Since then extensive studies were carried on these moments, and they have been applied in many fields such as: image analysis [5, 45, 71, 75–77], image watermarking [13, 60], pattern recognition [20, 56], edge detection [22, 24] and data compression [24]. Nevertheless, to our knowledge, image moments' transforms have not been yet explored in the area of image encryption.

Observing the excellent image representation capabilities of discrete moments, we are motivated to explore the capabilities of moments for image encryption. For that, in this paper, we introduce a new set of encryption algorithms based on chaos and operating in the transform domain of moments. We will focus particularly on the use of classical discrete orthogonal moments such as Tchebichef [45], Krawtchouk [71], Hahn [75], Dual-Hahn [77] and Racah [76]. We use two logistic chaotic maps for the encryption, an external key of 128 bits is divided in to two segments of equal size: K_1 and K_2, each 64 bits serve as the initial condition for the corresponding logistic map. After computing the moments' coefficients, an operation of confusion/diffusion is performed to obtain the cipher image. Decryption is the inverse process which allows to recover the original image from the cipher form. A set of experiments and tests are conducted: entropy, key space analysis, statistical and differential attacks are used in order to evaluate the performance of the proposed algorithms, then we compare them with the encryption on the frequency domain using DCT and state-of-the art algorithms presented in [11, 42].

The rest of this paper is organized as follows. Section 2 serves as a background study for orthogonal moments and chaos encryption. Section 3 presents the proposed schemes. The experimental results are illustrated in Section 4 and a conclusion is drawn in Section 5.

2 Theoretical background

2.1 Moment functions

First introduced by Hu [25] in 1961. Moments' invariants have found several applications [10, 14, 43] in image processing due to their ability to represent global features. However reconstructing the image is a difficult task because these moments are not orthogonal.

In 1980 Teague [57] has proposed moments with orthogonal basis functions such as Legendre and Zernike. These moments are able to store information with minimal information redundancy and have been extensively used in recent past [3, 22, 32]. Numerical approximation of continuous integrals, large variation in the dynamic range of values and coordinate space transformation are some common problems encountered when implementing these moments. The above problems motivated the researchers to consider the use of discrete orthogonal polynomials as the basis set, since the implementation of discrete orthogonal moments does not involve any numerical approximations, the basis functions satisfy the orthogonality property, and thus yield to a superior image representation [45].

2.1.1 Discrete orthogonal moments

For an $N \times M$ image with intensity function $f(x, y)$, the general formula of an $(n+m)$ order moment, can be expressed as:

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

Where NF is the normalization factor, $kernel_{nm}()$ is the moment's kernel which constitutes the orthogonal basis of a specific polynomials of order n and m. By changing the Kernel's polynomial we get different moments' families. Table 1 summarizes the main characteristics of the moments used in this paper.

The inverse transform function to reconstruct the original image is:

$$\tilde{f}(x, y) = \sum_{n=0}^{\eta_{max}} \sum_{m=0}^{\eta} kernel_{nm}(x, y) M_{nm} \tag{2}$$

Table 1 Main characteristics of discrete orthogonal moments

Moment family	$Kernel_{nm}(x, y)$	polynomial form	Normalization factor
Tchebichef [45]	$t_n(x) \times t_m(y)$	$t_n(x) = (1-N)_n\ {}_3F_2(-n, -x, 1+n; 1, 1-N; 1)$	$\frac{1}{\tilde{\rho}(p,N)\tilde{\rho}(q,N)}$
Krawtchouk [71]	$K_n(x; p_1, N) \times K_m(y; p_2, N)$	$K_n(x; p, N) = \sum_{k=0}^{N} a_{k,n,p} x^k$	1
Hahn [75]	$h_m^{\mu,\nu}(x, N) \times h_n^{\mu,\nu}(y, N)$	$h_n^{(u,v)}(x, N) = (N+\nu-1)_n (N-1)_n \times \sum_{k=0}^{n} (-1)^k \frac{(-n)_k(-x)_k(2N+\mu+\nu-n-1)_k}{(N+\nu-1)_k(N-1)_k} \frac{1}{k!}$	1
Dual Hahn [77]	$w_n^{(c)}(s, a, b) \times w_m^{(c)}(t, a, b)$	$w_n^{(c)}(s, a, b) = \frac{(a-b+1)_n(a+c+1)_n}{n!}\ {}_3F_2(-n, a-s, a+s+1; a-b+1, a+c+1; 1)$	1
Racah [76]	$u_n^{(\alpha,\beta)}(s, a, b) \times u_m^{(\alpha,\beta)}(t, a, b)$	$u_n^{\alpha,\beta}(s, a, b) = \frac{1}{n!}(a-b+1)_n(\beta+1)_n(a+b+\alpha+1)_n\ {}_4F_3\left(\begin{matrix} -n, \alpha+\beta+n+1, a-s, a+s+1 \\ \beta+1, a+1-b, a+b+\alpha+1 \end{matrix}; 1\right)$	1

Table 2 Similarities and differences between chaotic systems and cryptographic algorithms

Chaotic system	Cryptography algorithm
Phase space: set of real numbers	Phase space: set of integers
Iteration	Rounds
Parameters	Keys
Sensitivity to inital conditions and parameters	Diffusion

From a theoretical point of view, if all image moments are computed, one may recover a reconstructed image which will be identical to the original image with minimum reconstruction error [50]

In order to facilitate the computations of these moments, the authors in [47, 49, 54] studied their computational aspects: symmetry property and recursive formula are two aspects that decrease the computational cost. The reader is invited to visit these papers for greater details about the computational aspects of moments.

2.2 Chaos theory for cryptography

The use of Chaos theory in cryptography can be traced back to 1949. In his masterpiece, Shannon [55] stated that: “Good mixing transformations are often formed by repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc. . . .

In a good mixing transformation . . . functions are complicated, involving all variables in a sensitive way. A small variation of any one (variable) changes (the outputs) considerably”. Even though he doesn’t use the word chaos explicitly, he mentions the basic mechanism of stretch-and-fold used in chaotic-cryptography [21]. Since then, researchers studied different ways to use chaos into cryptography [4, 9, 21, 26, 44, 59].

Chaos based cryptosystems are widely used for practical applications due to their properties like sensitive dependence on initial conditions, control parameters and pseudorandom behavior [51, 52]. Meanwhile an important difference exists between cryptographic algorithms and chaotic maps, since the former operates in a discrete space while the latter has a meaning only on a continuum [52]. Table 2 summarizes the differences and the similarities between chaos and cryptography [53].

The general architecture of chaos-based cryptosystem [53] is illustrated by the typical block diagram in Fig. 1.

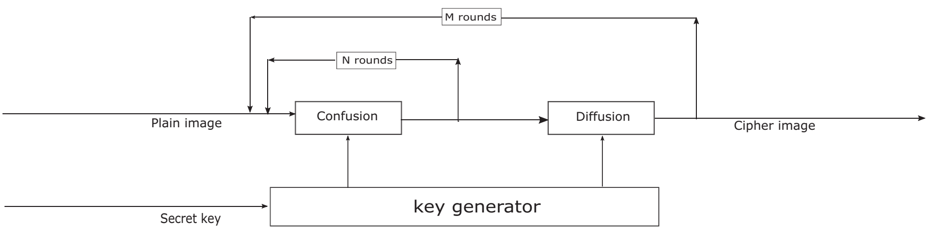

Fig. 1 Architecture of a chaos based cryptosystem [53]

In the confusion stage the pixels are permuted using a pseudo random sequence without changing the values of the image elements. This operation makes the image unrecognizable but it's not sufficient to make it secure [29]. The diffusion stage is where the values of each pixel are modified using the same or a different pseudo random sequence. These sequences are obtained by iterating a chaotic map. The confusion and the diffusion stages are repeated for a number of times to achieve a level of required security.

3 Proposed approach

We propose a set of novel encryption algorithms based on chaos and operating in the transform domain of discrete moments using: Tchebichef, Krawtchouk, Hahn, Dual-Hahn and Racah. In this section, we present in details the steps of the proposed image encryption procedures as well as the decryption process for each algorithm.

3.1 Encryption

The general scheme of the proposed algorithms is presented in Fig. 2. It comprises of three phases, namely: discrete moments' transform, confusion and diffusion. In the first stage, the moments' coefficients of the original image are calculated so that the image is represented in the transform domain of moments. In the confusion phase, positions of the pixels are changed without changing the actual values of the pixels, which destroys the affiliation among adjacent pixels and thus makes the image unrecognizable, the confusion stage is iterated N times, where N is typically greater than 1. In the diffusion stage the pixels' values are altered sequentially so that a small change in one pixel propagates to several pixels in order to hide the statistical structure of the plaintext image. The whole confusion-diffusion process repeats for M times to achieve a satisfactory level of security. The sequences used in the confusion and the diffusion stage are generated by two logistic maps with a seed secret key as input.

The logistic maps used are given by the equations:

$$x_{n+1} = \lambda x_n(1 - x_n), x\epsilon[0, 1] \tag{3}$$

$$y_{n+1} = \lambda y_n(1 - x_n), y\epsilon[0, 1] \tag{4}$$

Throughout the algorithm we keep $\lambda = 3.99$ which corresponds to a highly chaotic case while the initial conditions (X_0 and Y_0) are calculated using some mathematical manipulations explained in **step 1**. N and M are fixed to the minimal number of rounds 1, this makes the algorithm as fast as possible and as shown in the results section this does not affect the security performance of the algorithms.

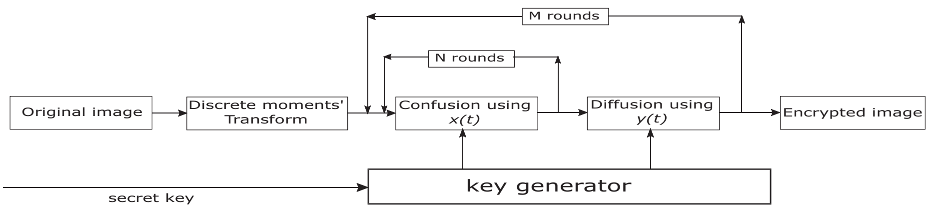

Fig. 2 Architecture of the proposed algorithms

step 1) Key generation: An external key of 128 bits is used, the key is divided in to two segments of equal size: K_1 and K_2, each 64 bits serve as the initial value for the corresponding logistic map. To adopt each segment as an initial value for the logistic map (a value between 0 and 1) we do some mathematical operations on the key:

We note each K_i in its binary representation: $K_1 = K_{11}K_{12}...K_{164}$; $K_2 = K_{21}K_{22}...K_{264}$, then the initial values of the two logistic maps are computed as follows:

$$X_0 = (K_{11} \times 2^0 + K_{12} \times 2^1 + ... + K_{164} \times 2^{63})/2^{64} \tag{5}$$

$$Y_0 = (K_{21} \times 2^0 + K_{22} \times 2^1 + ... + K_{264} \times 2^{63})/2^{64} \tag{6}$$

Where X_0 and Y_0 are the initial values of the first and the second logistic maps respectively.

step 2) Moments' computing: The difference between the proposed Tchebichef, Krawtchouk, Hahn, Dual Hahn and Racah based encryption algorithms is the moments' computation step, all the other steps are similar. In this step, we compute the moments' functions of the original image. For each proposed algorithm we compute the corresponding moments which constitute the orthogonal basis using the recursive formula discussed in section 2. In order to further optimize the moments' computations, we used the partitioning strategy proposed in [47]. Hence the image is divided into blocks of 8 x 8 and we compute the moments for these sub images, which enhances the moments' computation speed as we compute moments of low order. These moments' coefficients are stored in a matrix with the same size as the original image.

step 3) Confusion: In cryptographic terminology, confusion refers to the process of substitution. It is intended to make the relationship between the key and the ciphertext as complex as possible. In the proposed image encryption technique, we generate a random sequence of size 256*256 using the first logistic map with the initial condition X_0. Then transform the matrix obtained from step 2 into an array of size 256*256, which is permuted according to the sequence generated by the first logistic map.

step 4) Diffusion: Diffusion is the process of changing the statistical properties of the plain image by spreading the information in the plain image so that the redundancy is spread out over the cipher image. This process is required for a secure encryption technique. In fact, the diffusion process removes the vulnerability to differential attacks by comparing the plain and cipher images. In the diffusion stage the values of pixels are sequentially modified by the pseudo-random sequence generated by the chaotic map. In the proposed image encryption techniques, we generate another sequence from the second logistic map with initial condition Y_0, then a XOR operation is carried between the generated sequence and the array obtained in step 3.

step 5) The obtained array from step 4 is transformed back to a matrix of initial size 256*256 which is the final encrypted image.

3.2 Decryption

The decryption algorithm is similar to the encryption algorithm except that the steps are in reverse order as depicted in the Fig. 3. First the encrypted image is converted to an array of size 256*256. A XOR operation is then carried between the elements of the array and the random sequence early generated using Y_0 as its initial value. The elements of the resulted array are permuted according to the sequence which uses X_0 as its initial value. The resulting array is transformed back to a matrix of size 256*256. The inverse moments are computed using the appropriate moment's function (inverse DCT for the DCT based

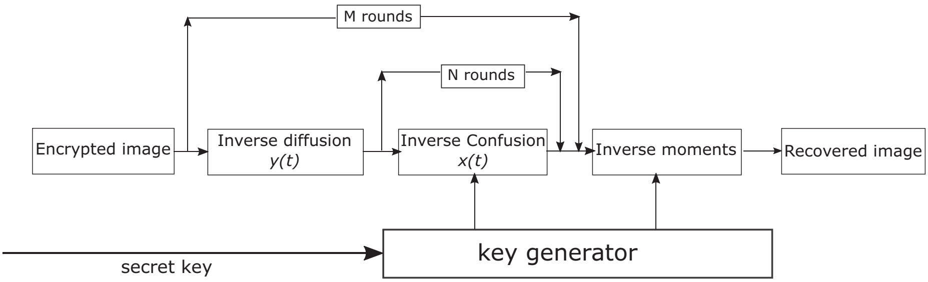

Fig. 3 Decryption scheme

encryption algorithm), thus we end up with the original image. Similarly to the encryption algorithm, we set M and N to 1.

4 Experimental results

An important issue of image encryption is evaluating the robustness of the algorithm in use. Visual inspection can be a clue, but we should not rely on it exclusively [18]. Other metrics had been proposed to judge the performance of the encryption algorithm more objectively [2, 15, 16, 39]. In order to validate the effectiveness of the newly introduced moments' based encryption schemes, a set of experiments is carried out and presented in four subsections. In the first subsection, the robustness to differential attacks is illustrated through NPCR and UACI parameters. In the second subsection, statistical attacks are addressed by studying the correlation coefficient. In the third subsection, the key space analysis is depicted. Finally we evaluate the security of the proposed algorithms in terms of entropy analysis. For each subsection we formally define the parameters used, then we present the results for the moments' based encryption algorithms and we compare them with DCT based encryption algorithm, and other state-of-the-art algorithms from refs [11, 42].

In this experimental study we use a set of twelve gray scale images of size 256*256 shown in Fig. 4. A subset of images composed of (D22, D35, D36, D41, D52, D66 and D67) is used to test the performance of the proposed algorithms on high textured images.

It is important to highlight that 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.

4.1 Differential attacks NPCR & UACI

We change one single pixel in the original image and evaluate its influence on the encrypted image. NPCR [67] (Number of Pixel Change Rate) is the difference of number of pixels between two encrypted images, UACI [67] (Unified Average Changing Intensity) is the difference between two encrypted images according to the average intensity. They are defined by formulas (7) and (8) respectively:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{7}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{8}$$

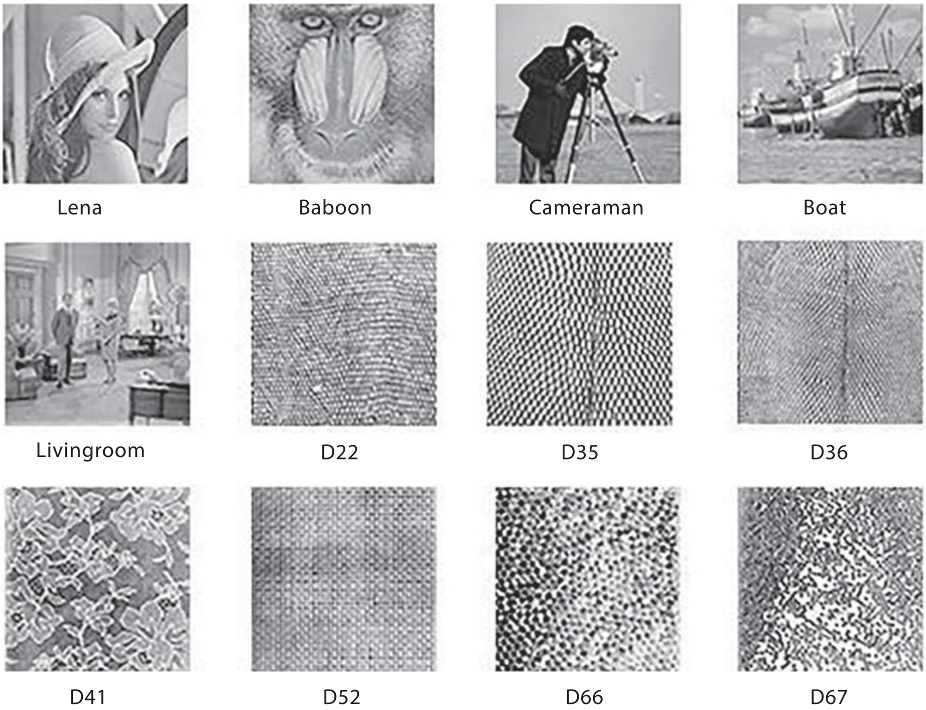

Fig. 4 Test images

W and H are the width and the height of the encrypted image. $C_1(i, j)$ and $C_2(i, j)$ are the pixel values at position (i,j) for the first and the second encrypted image respectively. If $C_1(i, j) \neq C_2(i, j)$, then $D(i, j) = 1$, otherwise $D(i, j) = 0$. The more the NPCR and UACI gets larger the more the algorithm is secure to the differential attacks [67].

Table 3 Comparative results in terms of NPCR values of test images

NPCR	Tchebichef	Krawtchouk	Racah	Hahn	Dual Hahn	DCT	Ref [42]	Ref [11]
Lena	99,791	99,7559	99,7086	99,7879	99,7864	99,7864	99,6329	99,5682
Baboon	99,7955	99,8337	99,7482	99,855	99,7391	99,7864	99,5696	99,6802
cameraman	99,7574	99,7437	99,6979	99,8276	99,7406	99,791	99,6949	99,5318
Boats	99,7589	99,7681	99,7253	99,8337	99,7726	99,7681	99,7507	99,6125
Livingroom	99,8093	99,7467	99,7284	99,8276	99,7711	99,8199	99,68	99,7854
D22	99,8306	99,7833	99,7604	99,831	99,8108	99,7986	99,6268	99,7006
D35	99,8093	99,7971	99,7604	99,8177	99,7223	99,7879	99,7498	99,657
D36	99,8093	99,7772	99,7925	99,8367	99,7833	99,7971	99,5788	99,6617
D41	99,8459	99,8047	99,7818	99,8276	99,7787	99,794	99,6139	99,6902
D52	99,8383	99,8032	99,7787	99,8199	99,8047	99,8047	99,7335	99,8131
D66	99,8154	99,7772	99,791	99,8337	99,7772	99,7971	99,7371	99,5863
D67	99,7894	99,762	99,7742	99,8032	99,7986	99,7971	99,6837	99,7799

In order to evaluate the security of the proposed algorithms against differential attacks. We compute NPCR and UACI for each cipher image for all the proposed algorithms and we compare them with the encryption algorithm based on DCT and the algorithms in [11, 42]. Thus the images presented in the Fig. 4 are encrypted using the encryption algorithms based on: Tchebichef, Krawtchouk, Racah, Hahn and dual Hahn moments and compared to the algorithm based on DCT and the encryption schemes in [11, 42], then the corresponding results are illustrated in Tables 3 and 4.

Examining the Table 3, it is clear that the Hahn based encryption algorithm has the higher values of NPCR for the majority of images (except for D41 and D52 where Tchebichef based encryption algorithm shows better results) which indicates that the Hahn based encryption algorithm exhibit good performance for NPCR.

In Table 4 we show the results for UACI. We see that the moments' based encryption algorithms exhibit satisfying results, the Krawtchouk based encryption algorithm clearly performs better for all images. Moreover, one can observe that all the moments based algorithms performs better on the more textured images (D22, D35, D36, D41, D52, D66 and D67).

As a main conclusion of these two experiments, the moments' based algorithms performs significantly better than the DCT based encryption algorithm and the encryption schemes in refs [11, 42] particularly on high textured images.

4.2 Correlation coefficient analysis

Correlation coefficient is a statistical test that measures the dependence and the similarity between the plain image and the cipher image. It takes a value between -1 and +1, 0 correlation indicates that there is no correlation between the two images. A correlation of 1 means that the original and the encrypted images are in perfect correlation and there is a high dependence between the two images. Thus, for a good encryption algorithm the correlation coefficient should be near to zero [1].

Table 4 Comparative results in terms of UACI values of test images

UACI	Tchebichef	Krawtchouk	Racah	Hahn	Dual Hahn	DCT	Ref [42]	Ref [11]
Lena	29,158	32,249	27,242	28,659	26,977	30,3256	30,638	31,313
Baboon	30,44	31,773	26,271	26,813	24,35	24,6456	30,17	28,846
cameraman	26,301	29,435	23,221	27,54	25,492	27,6376	27,61	26,768
Boats	25,102	27,503	21,287	25,609	21,389	26,3152	26,455	26,657
Livingroom	28,157	30,979	24,224	26,703	23,111	26,024	29,61	25,349
D22	33,617	34,55	32,651	30,36	30,371	29,496	29,537	33,164
D35	33,381	34,636	31,521	29,834	29,247	28,7616	26,283	31,002
D36	33,309	34,651	32,594	30,434	30,921	28,2256	26,489	31,366
D41	33,156	34,819	32,555	30,986	31,567	29,4944	28,162	27,707
D52	33,779	34,254	33,538	29,86	30,298	28,1968	27,501	30,603
D66	33,758	34,748	31,657	29,748	29,772	28,564	28,833	27,144
D67	33,81	34,27	32,593	30,712	30,57	30,9352	26,323	28,375

The correlation coefficient C.C is computed between the plain image x and the cipher image y, when arranged as one-dimensional sequences as follows [46]:

$$C.C = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{9}$$

Where $cov(x, y) = \frac{1}{L}\sum_{l=1}^{L}(x(l) - E(x))(y(l) - E(y))$, $D(x) = \frac{1}{L}\sum_{l=1}^{L}(x(l) - E(x))^2$, $E(x) = \frac{1}{L}\sum_{l=1}^{L} x(l)$ and L is the total number of pixels in the image.

In order to evaluate the robustness of the proposed moments' based encryption algorithms, we compute the correlation coefficient using formula (9) between the plain images and their corresponding ciphers. We encrypt each image in the image test set using Tchebichef, Krawtchouk, Racah, Hahn and dual Hahn based encryption algorithms and we compare the results with DCT encryption based algorithm and the algorithms in [11, 42]. The results obtained are presented in Table 5.

Based on the results provided by Table 5, it can be seen that the correlation coefficient is near to zero for all encryption algorithms which suggests that the implemented algorithms have a good quality of encryption. In addition the experimental results demonstrates that the Hahn based encryption algorithms is relatively more effective than the other algorithms including DCT and the state-of-the-art algorithms.

4.3 Key space analysis

For a secure image cipher, the key space should be large enough to make the brute force attack infeasible. The proposed image cipher has $2^{128} \sim 3.4028 \times 10^{38}$ different combinations of the secret key. An image cipher with such a long key space is sufficient for reliable practical use.

4.4 Entropy analysis

Entropy is a measure used for evaluating the security of an image encryption algorithm, it shows the degree of unpredictability and randomness in a system [17]. A good

Table 5 Comparative results in terms of Correlation coefficient of test images

C.C	Tchebichef	Krawtchouk	Racah	Hahn	Dual Hahn	DCT	Ref [42]	Ref [11]
Lena	0,00043491	-0,0063	0,0021	0,00046734	0,0036	0,0021	-0,0023	0,004
Baboon	0,0066	0,0098	-0,0015	0,0037	0,0064	-0,0044	0,0071	0,0074
cameraman	0,0046	-0,00075892	0,0034	-0,0018	0,0019	0,0054	-0,0091	0,0071
Boats	-0,0029	-0,0102	0,0022	-0,0024	0,00023248	0,0029	-0,0052	0,0087
Livingroom	-0,0012	-0,0041	-0,0023	0,00097113	-0,001	-0,0033	0,0033	0,0027
D22	0,0051	0,0022	0,0053	0,0017	0,0076	-0,0049	-0,0096	-0,0081
D35	-0,004	-0,0012	0,00056295	-0,0007745	-0,0057	-0,001	0,0017	-0,0054
D36	-0,0052	-0,0066	-0,002	-0,0019	-0,0062	-0,0027	-0,0034	-0,0041
D41	-0,000018699	0,0038	0,0078	0,001	0,0055	0,0016	-0,0059	0,0037
D52	-0,0081	-0,00010628	-0,007	-0,0032	-0,0034	0,0038	0,0053	-0,0091
D66	0,00058458	-0,0025	-0,0041	-0,0043	-0,0014	-0,0052	-0,0056	-0,0054
D67	-0,0036	-0,0049	-0,0017	-0,0048	-0,0069	-0,0066	0,0073	0,0064

Table 6 Comparative results in terms of entropy of test images

Entropy	Tchebichef	Krawtchouk	Racah	Hahn	Dual Hahn	DCT	Ref [42]	Ref [11]
Lena	7,9946	7,9953	7,9955	7,9955	7,9953	7,9945	7,9943	7,9946
Baboon	7,995	7,9956	7,9958	7,9956	7,9952	7,9948	7,9945	7,9944
cameraman	7,9944	7,9953	7,9955	7,9955	7,9951	7,9947	7,9938	7,9934
Boats	7,9946	7,9954	7,9955	7,9956	7,9953	7,9949	7,994	7,9943
Livingroom	7,9945	7,9953	7,9955	7,9956	7,9953	7,9949	7,9943	7,9933
D22	7,9952	7,9957	7,9958	7,9954	7,9954	7,9952	7,9951	7,995
D35	7,9952	7,9956	7,9959	7,9957	7,9955	7,9949	7,9929	7,9944
D36	7,9955	7,9955	7,9957	7,9955	7,9955	7,9951	7,9936	7,9945
D41	7,9953	7,9956	7,9957	7,9956	7,9956	7,9951	7,9938	7,9947
D52	7,9954	7,9956	7,9958	7,9956	7,9956	7,9947	7,9944	7,9947
D66	7,9955	7,9956	7,9957	7,9954	7,9954	7,9952	7,9952	7,9949
D67	7,9954	7,9955	7,9957	7,9956	7,9956	7,9953	7,9949	7,9944

encryption algorithm should decrease the mutual information among pixels, and thus increase the entropy. The entropy $H(m)$ of any message m is given by the formula :

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)} \tag{10}$$

Where $p(m_i)$ is the probability of occurrence of symbol m_i. A perfect image encryption – if it exists- should have the entropy value of 8 and is considered to provide no information about the original image [40].

To demonstrate the security of the proposed methods in regard to the entropy measure. We encrypt each image depicted in Fig. 4, using Tchebichef, Krawtchouk, Racah, Hahn and dual Hahn based encryption algorithms, we compute the entropy of the cipher images and we compare the results with the obtained entropy of the DCT encryption based algorithm and the algorithms in [11, 42]. The results are depicted in Table 6.

The results presented in Table 6 clearly show that all the implemented algorithms give a high value of entropy i.e. close to 8, which exhibits a high efficiency of these algorithms. Furthermore, it's worth mentioning that most of the moments' based encryption algorithms outperform the encryption algorithm based on DCT and state-of-the-art algorithms, especially for the highly textured images namely D22, D35, D36, D41, D52, D66 and D67.

5 Conclusion

In this paper, we have proposed a new set of image encryption algorithms based on discrete orthogonal moments combined with chaos theory. Several experiments have been used for measuring the encryption quality of the proposed algorithms. We performed a comparison with a similar algorithm operating in DCT domain and some state-of-the-art algorithms in terms of entropy, key space analysis differential and statistical attacks. It should be mentioned that in most experiments, the proposed algorithms gives satisfying results and outperform the DCT based encryption algorithm and the state-of-the-art methods specially for highly textured images.

As a conclusion, given all presented performances of this new set of algorithms, we are confident about their ability to be used in real world scenarios for image encryption. Thus, in our future works, we will focus on presenting a fast algorithm for real time video encryption based on discrete orthogonal moments.

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

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

Compliance with Ethical Standards

Conflict of interests The authors declare no conflict of interest.

References

1. Ahmad J, Hwang SO, Ali A (2015) An experimental comparison of chaotic and non-chaotic image encryption schemes. Wirel Pers Commun 84(2):901–918
2. Ahmed HEDH, Kalash HM, Allah OF (2007) Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images. In: International conference on electrical engineering, 2007. ICEE'07. IEEE, pp 1–7
3. Bailey RR, Srinath M (1996) Orthogonal moment features for use with parametric and non-parametric classifiers. IEEE Trans Pattern Anal Mach Intell 18(4):389–399
4. Baptista M (1998) Cryptography with chaos. Phys Lett A 240(1-2):50–54
5. Batioua I, Benouini R, Zenkouar K, El Fadili H (2017) Image analysis using new set of separable two-dimensional discrete orthogonal moments based on racah polynomials. EURASIP J Image Video Process 2017(1):20
6. Batioua I, Benouini R, Zenkouar K, Zahi A et al (2017) 3d image analysis by separable discrete orthogonal moments based on krawtchouk and tchebichef polynomials. Pattern Recogn 71:264–277
7. Benouini R, Batioua I, Zenkouar K, Najah S, Qjidaa H (2018) Efficient 3d object classification by using direct krawtchouk moment invariants. Multimed Tools Appl, p 1–26
8. Benouini R, Batioua I, Zenkouar K, Zahi A, Najah S, Qjidaa H (2019) Fractional-order orthogonal chebyshev moments and moment invariants for image representation and pattern recognition. Pattern Recogn 86:332–343
9. Bianco ME, Reed DA (1991) Encryption system based on chaos theory. US Patent 5,048,086
10. Casasent D, Cheatham RL (1984) Image segmentation and real-image tests for an optical moment-based feature extractor. Optics commun 51(4):227–230
11. Chai X, Chen Y, Broyde L (2017) A novel chaos-based image encryption algorithm using dna sequence operations. Optics and Lasers in Engineering 88:197–213
12. Chen CS, Chen RJ (2006) Image encryption and decryption using scan methodology. In: Seventh international conference on parallel and distributed computing, applications and technologies, 2006. PDCAT'06. IEEE, pp 61–66
13. Deng C, Gao X, Li X, Tao D (2009) A local tchebichef moments-based robust image watermarking. Signal Process 89(8):1531–1539
14. Dudani SA, Breeding KJ, McGhee RB (1977) Aircraft identification by moment invariants. IEEE Trans Comput 100(1):39–46
15. El-Ashry I (2010) Digital image encryption. MS. c Thesis, Electronics and Electrical Communications Engineering Dept., Faculty of Electronic Engineering Menofia University
16. El Fishawy NF, Zaid OMA (2007) Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms. IJ Network Security 5(3):241–251
17. El-Wahed MA, Mesbah S, Shoukry A (2008) Efficiency and security of some image encryption algorithms. In: Proceedings of the world congress on engineering, vol 1, pp 2–4. London

18. Elkamchouchi H, Makar M (2005) Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers. In: Radio science conference, 2005. NRSC 2005. Proceedings of the twenty-second national, pp 277–284. IEEE
19. Enayatifar R, Abdullah AH, Lee M (2013) A weighted discrete imperialist competitive algorithm (wdica) combined with chaotic map for image encryption. Opt Lasers Eng 51(9):1066–1077
20. Flusser J, Suk T (1993) Pattern recognition by affine moment invariants. Pattern Recogn 26(1):167–174
21. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos 8(06):1259–1284
22. Ghosal S, Mehrotra R (1993) Orthogonal moment operators for subpixel edge detection. Pattern Recogn 26(2):295–306
23. Guan M, Yang X, Hu W (2019) Chaotic image encryption algorithm using frequency-domain dna encoding. IET Image Process 13(9):1535–1539
24. Hsu HS, Tsai WH (1993) Moment-preserving edge detection and its application to image data compression. Optical Eng 32(7):1596–1609
25. Hu MK (1962) Visual pattern recognition by moment invariants. IRE Trans Inform Theory 8(2):179–187
26. Hua Z, Zhou Y, Huang H (2019) Cosine-transform-based chaotic system for image encryption. Inf Sci 480:403–419
27. Hussain I, Shah T, Gondal MA (2012) An efficient image encryption algorithm based on s8 s-box transformation and nca map. Opt Commun 285(24):4887–4890
28. Jiang NZX, Lan X (2006) Advances in machine vision, image processing and pattern analysis
29. Jolfaei A, Wu XW, Muthukkumarasamy V (2016) On the security of permutation-only image encryption schemes. IEEE Trans Inform Forensics Secur 11(2):235–246
30. Khan JS, Ahmad J (2019) Chaos based efficient selective image encryption. Multidim Syst Sign Process 30(2):943–961
31. Khotanzad A, Hong YH (1990) Invariant image recognition by zernike moments. IEEE Trans Pattern Anal Mach Intell 12(5):489–497
32. Khotanzad A, Liou JH (1996) Recognition and pose estimation of unoccluded three-dimensional objects from a two-dimensional perspective view by banks of neural networks. IEEE Trans Neural Netw 7(4):897–906
33. Kotulski Z, Szczepański J (1997) Discrete chaotic cryptography. Ann Phys 509(5):381–394
34. Leng L, Zhang J, Khan MK, Chen X, Alghathbar K (2010) Dynamic weighted discrimination power analysis: a novel approach for face and palmprint recognition in dct domain. Int J Phys Sci 5(17):2543–2554
35. Leng L, Zhang J, Xu J, Khan MK, Alghathbar K (2010) Dynamic weighted discrimination power analysis in dct domain for face and palmprint recognition. In: 2010 international conference on information and communication technology convergence (ICTC). IEEE, pp 467–471
36. Li C, Luo G, Qin K, Li C (2017) An image encryption scheme based on chaotic tent map. Nonlinear Dynamics 87(1):127–133
37. Li S, Chen G, Cheung A, Bhargava B, Lo KT (2007) On the design of perceptual mpeg-video encryption algorithms. IEEE Trans Circ Sys Video Technol 17(2):214–223
38. Li S, Li C, Chen G, Zhang D, Bourbakis NG (2004) A general cryptanalysis of permutation-only multimedia encryption algorithms. IACR's Cryptology ePrint Archive: Report 374:2004
39. Lian S (2008) Multimedia content encryption: techniques and applications. Auerbach Publications
40. Liang J, Shi Z (2004) The information entropy, rough entropy and knowledge granulation in rough set theory. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 12(01):37–46
41. Liu S, Guo C, Sheridan JT (2014) A review of optical image encryption techniques. Optics & Laser Technology 57:327–342
42. Luo Y, Du M, Liu J (2015) A symmetrical image encryption scheme in wavelet and time domain. Commun Nonlinear Sci Numer Simul 20(2):447–460
43. Markandey d. (1992) Robot sensing techniques based on high-dimensional moment invariants and tensors. IEEE Trans Robotics Automation 8(2):186–195
44. Matthews R (1989) On the derivation of a chaotic encryption algorithm. Cryptologia 13(1):29–42
45. Mukundan R, Ong S, Lee PA (2001) Image analysis by tchebichef moments. IEEE Trans Image Process 10(9):1357–1364
46. Naeem EA, Elnaby MMA, El-sayed HS, El-Samie FEA, Faragallah OS (2016) Wavelet fusion for encrypting images with a few details. Comput Electrical Eng 54:450–470
47. Nakagaki K, Mukundan R (2007) A fast 4x4 forward discrete tchebichef transform algorithm. IEEE Signal Process Lett 14(10):684–687
48. Padilla-López JR, Chaaraoui AA, Flórez-Revuelta F (2015) Visual privacy protection methods: a survey. Expert Syst Appl 42(9):4177–4195

49. Papakostas GA, Karakasis EG, Koulouriotis DE (2008) Efficient and accurate computation of geometric moments on gray-scale images. Pattern Recogn 41(6):1895–1904
50. Papakostas GA, Koulouriotis DE, Karakasis EG (2010) Computation strategies of orthogonal image moments: a comparative study. Appl Math Comput 216(1):1–17
51. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image and Vision Comput 24(9):926–934
52. Radwan AG, AbdElHaleem SH, Abd-El-Hafiz SK (2016) Symmetric encryption algorithms using chaotic and non-chaotic generators: a review. J Adv Res 7(2):193–208
53. Sankpal PR, Vijaya P (2014) Image encryption using chaotic maps: a survey. In: 2014 fifth international conference on signal and image processing (ICSIP). IEEE, pp 102–107
54. See K, Loke KS, Lee P, Loe KF (2007) Image reconstruction using various discrete orthogonal polynomials in comparison with dct. Appl Math Comput 193(2):346–359
55. Shannon CE (1949) Communication theory of secrecy systems. Bell System Technical Journal 28(4):656–715
56. Suk T, Flusser J (2003) Combined blur and affine moment invariants and their use in pattern recognition. Pattern Recogn 36(12):2895–2907
57. Teague MR (1980) Image analysis via the general theory of moments. JOSA 70(8):920–930
58. Tedmori S, Al-Najdawi N (2014) Image cryptographic algorithm based on the haar wavelet transform. Inf Sci 269:21–34
59. Teh JS, Alawida M, Sii YC (2020) Implementation and practical problems of chaos-based cryptography revisited. J Inform Secur Appl 102421:50
60. Tsougenis E, Papakostas GA, Koulouriotis DE (2015) Image watermarking via separable moments. Multimed Tools Appl 74(11):3985–4012
61. Wallin Å, Kubler O (1995) Complete sets of complex zernike moment invariants and the role of the pseudoinvariants. IEEE Trans Pattern Anal Mach Intell 17(11):1106–1110
62. Wang C, Wang X, Xia Z, Ma B, Shi YQ (2019) Image description with polar harmonic fourier moments. IEEE Trans Circ Sys Video Technol
63. Wang W, Si M, Pang Y, Ran P, Wang H, Jiang X, Liu Y, Wu J, Wu W, Chilamkurti N et al (2018) An encryption algorithm based on combined chaos in body area networks. Comput Electrical Eng 65:282–291
64. Wang W, Tan H, Sun P, Pang Y, Ren B (2016) A novel digital image encryption algorithm based on wavelet transform and multi-chaos. In: Wireless communication and sensor network: proceedings of the international conference on wireless communication and sensor network (WCSN 2015), pp 711–719. World Scientific
65. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
66. Wu J, Guo F, Zeng P, Zhou N (2013) Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence. J Mod Opt 60(20):1760–1771
67. Wu Y, Noonan JP, Agaian S (2011) Npcr and uaci randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. Journal of Selected Areas in Telecommunications (JSAT) 1(2):31–38
68. Xin G, Fen-lin L, Bin L, Wei W, Juan C (2010) An image encryption algorithm based on spatiotemporal chaos in dct domain. In: 2010 the 2nd IEEE international conference on information management and engineering (ICIME). IEEE, pp 267–270
69. Xiong Z, Wu Y, Ye C, Zhang X, Xu F (2019) Color image chaos encryption algorithm combining crc and nine palace map. Multimed Tools Appl 78(22):31035–31055
70. Xu L, Gou X, Li Z, Li J (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt Lasers Eng 91:41–52
71. Yap PT, Paramesran R, Ong SH (2003) Image analysis by krawtchouk moments. IEEE Trans Image Process 12(11):1367–1377
72. Ye G, Huang X (2018) Spatial image encryption algorithm based on chaotic map and pixel frequency. Sci China Inform Sci 61(5):058104
73. Ye G, Pan C, Huang X, Mei Q (2018) An efficient pixel-level chaotic image encryption algorithm. Nonlinear Dynamics, pp 1–12
74. Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284(12):2775–2780
75. Zhou J, Shu H, Zhu H, Toumoulin C, Luo L (2005) Image analysis by discrete orthogonal hahn moments. In: International conference image analysis and recognition. Springer, pp 524–531
76. Zhu H, Shu H, Liang J, Luo L, Coatrieux JL (2007) Image analysis by discrete orthogonal racah moments. Signal Process 87(4):687–708

77. Zhu H, Shu H, Zhou J, Luo L, Coatrieux JL (2007) Image analysis by discrete orthogonal dual hahn moments. Pattern Recogn Lett 28(13):1688–1704

Abdelhalim Kamrani He received a M.S. degree in Intelligent Systems and Networks, from the Faculty of Science and Technology, University of Sidi Mohammed Ben Abdellah, Fez, Morocco in 2016. He is currently pursuing his Ph.D. degree in Computer Science at the Faculty of Science and Technology of Fez. His research interests include data encryption and image analysis.

Khalid Zenkouar He received a Ph.D. degree in image analysis from Faculty of Science, University Sidi Mohamed Ben Abdellah, Fez, Morocco in 2006. Now he is a professor of the Department of computer engineering, Faculty of Science and Technology Fez Morocco. He is a member in the LSIA Laboratory (Laboratory of Intelligent Systems and Application). His current research interests include image analysis, machine intelligence and pattern recognition.

Said Najah He received a Ph.D. degree in Computer Science from the Faculty of Science, University Sidi Mohamed Ben Abdellah, Fez, Morocco in 2006. He is currently a professor of the Department of Computer Science, Faculty of Science and Technology Fez Morocco. He is a member in the LSIA Laboratory (Laboratory of Intelligent Systems and Application). His current research interests include parallel computing, big data analytics and artificial intelligence.