*International Journal For Technological Research In Engineering* *ISSN (Online): 2347 - 4718*
*International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - November 2016)*

# SIMULTANEOUS ENCRYPTION AND COMPRESSION USING CHAOTIC KICKED ROTATOR MAP – DRPE WITH DIRECTION ADAPTIVE DISCRETE WAVELET TRANSFORM

R.Sivamalar[1], Dr.Swati Sharma[2]
[1]Lecturer, Department of Computer Science and Information System, Jazan University, Ministry of Higher Education, Jazan, Kingdom of Saudi Arabia.
[2]Department of Electrical Engineering, Jodhpur National University, Jodhpur, Rajasthan, India.Designation

***Abstract: Significant work has been done in the areas of optical image encryption and compression as two independent problems, yet the two areas are strongly interleaved and should be considered simultaneously. Consider that current practice in image processing generally uses encryption on compressed image data or attempts to compress data that has already been encrypted. However, it is generally seen that traditional encryption techniques degrades compression. In this paper, we propose a method which prepares an image for compression while simultaneously encrypting the image data. The simultaneous compression and encryption of optical images is done by introducing Direction-Adaptive Discrete Wavelet Transform compression (DADWTC) and utilizing it with the combination of CKRMDRPE thus forming the simultaneous encryption and compression scheme called CKRMDRPE-DADWTC. In this scheme, CKRMDRPE encrypts the optical image while DADWTC simultaneously compressing it. The experimental results show that the proposed CKRMDRPE-DADWTC provides better results in terms of bandwidth, throughput, latency and error rate.***

***Keywords: Optical image Encryption and Compression, Chaotic Kicked Rotator Map with Double Random Phase Encoding (CKRMDRPE), Direction-Adaptive Discrete Wavelet Transform compression (DADWTC)***

## I. INTRODUCTION

OPTICALimages are subject to various attacks by the hackers while transmission. This problem can be solved by applying encryption of optical images. Optical encryption can provide a better and safer image communication. In order to receive and retrieve the original optical information at the receiver side, robust encryption scheme is needed. Optical information hiding techniques have received significant attention recently, because of their considerable potential advantages, such as their inherent capabilities for parallel ultra-fast processing, and the possibility of their applications in biometrics [1], optical security [2] and product authenticity verification [3]. Using these techniques, information can be hidden or secured in a large number of different kinds of dimensions offering many degrees of freedom. In 1995 Refregier and Javidi [2] proposed the double random phase encoding (DRPE) method to encode an amplitude image into a stationary white noise pattern. This includes multiplication of the image by random phase screens both in the input (space) and Fourier (spatial frequencies) planes. Fully phase-based encryption (PE) provides much better performance than linear amplitude-based (AE) encryption because of the secure properties of non linear PE [4]. Several other algorithms, for instance, digital optical stream cipher [5], optical XOR image encryption [6], and information encryption with phase-shifting interferometry [7], have yielded theoretical and experimental results that indicate a high level of security can be achieved by applying optically inspired hiding techniques. An early work of optical image encryption, chaotic Baker map and Double Random Phase Encoding (DRPE) is presented in [8]. This technique is implemented in two layers to enhance the security level of the classical DRPE. The first layer is a pre-processing layer, which is performed with the chaotic Baker map on the original image. In the second layer, the classical DRPE is utilized. However, the Chaotic Baker Map has low speed problem and number representation problems due to the utilization of floating point values over other number representations. Hence the Chaotic Baker Map is replaced by the efficient Chaotic Kicked rotator map which reduces the computation complexities and the speed problem by utilizing the bit-wise representation of the numbers. Thus the proposed CKRMDRPE enhances the security with efficient results. The strength of the CKRMDRPE and CBMDRPE are tested by a known plain test attack which uses ant colony optimization for key estimation it is observed that cipher text can be decrypted in CBMDRPE while cannot be decrypted while utilizing CKRMDRPE.

During transmission of encrypted optical images, it requires high bandwidth and this issue also occurs in CKRMDRPE. In order to overcome this drawback simultaneous encryption and compression of optical images has to be performed. DADWTC provides optical image compression and hence it is implemented with CKRMDRPE to form the simultaneous encryption and compression scheme called CKRMDRPE-DADWTC. This approach enhances the security of the optical images while the bandwidth used for transmission is reduced.

## II. RELATED WORKS

Zhou, N., & Dong, T., [9] proposed image encryption scheme based on multiple-parameter random fractional Fourier transform (MPRFrFT). The MPRFrFT algorithm inherits virtues from MPFrFT and RFrFT with multi-parameter such as fractional order, period, arbitrary integer vectors of MPFrFT and random phase mask of RFrFT. The attackers cannot obtain the valid information without correct keys. Decrypt key fractional order value is required is high.

Lai, J., et al [10] proposed an encryption algorithm based on fractional Fourier transform and Chaotic system. In this method image encryption includes two steps. Initially image is encrypted by fractional Fourier double random phase transform then confusion image is encrypted by confusion matrix which is generated by chaotic system and thus chipper image is obtained. But the security is depends on the sensitivity to randomness of phase mask, the orders of FRFT and initial conditions of chaotic system.

Liu, Z., et al [11] proposed image encryption based on random rotation operation in fractional Fourier transform domains. The rotation operation includes rotation of center, radii and angle. For data of amplitude and phase of complex number rotation operation is performed with random controlling parameters. But encrypted data is very sensitive for data change which will be amplified iterative process.

Liu, S., & Sheridan. J. T., [12] proposed an encryption by combining image scrambling techniques in fractional Fourier transform. Hiding of information in two-dimensional images is done by combining image scrambling techniques in fractional Fourier transform. Initially image is randomly shifted by jigsaw transform algorithm and pixel scrambling is applied based on Arnold transform (ART). Then scrambled image is encrypted by using fractional Fourier transform.

## III. REVIEW OF OUR PREVIOUS STUDY

### 3.1 Chaotic Kicked Rotator Map & Double Random Phase Encoding (CKRMDRPE)

CKRMDRPE replaces the chaotic baker map with chaotic kicked rotator map. CKRM utilizes bit-wise representation of numbers so that the speed problems do not occur while the computation complexity is also reduced. CKRM can be described by employing the two-dimensional maps M. The variables p and q are considered which appear as canonical coordinate and momentum. The (p,q) plane and the phase space are mapped onto itself.

$$\bar{p} = f(p,q)$$
$$\bar{q} = g(p,q)$$

The mapping in M can be described as

$$(p,q) \overset{M}{\rightarrow} (\bar{p},\bar{q})$$

The mapping M is area preserving, the Jacobian determinant J that relates the phase space areas

$\Delta\bar{p}\Delta\bar{q} = J\Delta p\Delta q$is equal to unity

$$J = \left|\frac{\partial(\bar{p},\bar{q})}{\partial(p,q)}\right| = 1$$

Initializing at the point $(p_0, q_0)$ and iterating the map, generates the sequence of points $(p_n, q_n), n = 0,1,2, \ldots$.

The consideration of delta-kicked rotator with the Hamiltonian system can resolve the chaotic map.

$$H = \frac{p^2}{2m} + \delta_\tau(t)K\cos q$$

Where $\delta_\tau(t)$ is the $\tau$-th periodic comb function, its value is non-zero only at a periodic sequence of delta-spikes.

$$\delta_\tau(t) = \sum_{n=-\infty}^{+\infty} \delta(\frac{t}{\tau} - n)$$

The chaotic kicked rotator system can be written as

$$H(p,q,t) = T(p) + \delta_\tau(t)V(q)$$

Where $V(q) = kq^2$ is the potential of the particle in map
Considering the angular momentum, the chaotic kicked rotator becomes

$$\bar{p} = p + K\sin q$$
$$\bar{q} = q + \bar{p}$$

The dimensionless parameter K is the measure of the kick strength and is proportional to the ratio of the potential energy of the field, dE, and the rotational energy for rotation in resonance with the period of kicks. It is given by

$$K = \tau^2 dE/I$$

Where I is the moment of inertia

When applying additional scaling, the chaotic kicked rotator becomes

$$\bar{p} = p + \frac{K}{2\pi}\sin 2\pi q$$
$$\bar{q} = q + \bar{p}$$

Where q is taken modulo one in the interval $0 \le q < 1$

Using this chaotic kicked rotator, the encryption process can be written as

$$\psi_B(x,y) = FT^{-1}[FT\big(f_B(x,y)\varphi_n(x,y)\big)\varphi_m(\bar{p},\bar{q})]$$

While the decryption process can be written as

$$FT^{-1}[FT(\psi_B(x,y)\varphi_m^*(\bar{p},\bar{q})] = f_B(x,y)\varphi_n(x,y)$$

3.2 Known-plaintext attack

Known-plaintext attack is one way to test the strength of an encryption algorithm. In known-plaintext cryptanalysis, the attacker has a priori knowledge of the encryption mechanism as well as a plaintext and cipher text pair. If the attacker is able to find the key used for a given plaintext-cipher text pair, then the security of all the past and future cipher texts, which used the same key, can be easily identified. Let us assume that the attacker tries to decrypt a cipher text encrypted using Fourier plane encoding by the blind decryption method. In this method, he tries to decrypt the cipher text by randomly picking a key from the key space, and compares the resulting 'decrypted' plain text to the original plaintext. The probability of finding the correct mask in t searches would be approximately tK−1 where K is the size of the key space. For an N ×N pixel encryption phase mask with m phase levels, the key space is as large as K = mN×N. If one considers that some fraction $r(\varepsilon) \in [0,1]$of the keys could give a decryption with some acceptable error$\varepsilon$, then the probability of finding one of these (estimated) keys increases to t $(r(\varepsilon)K)^{-1}$for a particular$\varepsilon$. If the attacker finds anyone of these estimated keys he would decrypt the cipher text with some error. ACO algorithm to find a phase masks which would approximately decrypt the cipher text $\psi$ (.) to give an estimated plaintext f̃. A system with a phase-key that has N * M pixels, each with Q quantization levels, has Q (N*M) keys. ACO algorithms have advantage over simulated annealing when the graph may change dynamically, the ant colony algorithms can be run continuously and adapt to changes in real time. Thus the most effective key is estimated using ACO. The cost value E is calculated as the NRMS error between the decrypted image and the original plaintext image. The normalized root mean squared (NRMS) error is equal to or less than some threshold ε. The NRMS error is calculated as

$$NRMS = \sqrt{\frac{\sum_{i=1}^{n}\sum_{j=1}^{n}|I_d(i,j) - I(i,j)|^2}{\sum_{i=1}^{n}\sum_{j=1}^{n}|I(i,j|)^2}}$$

where$I_d(.)$ =|f̃ |2 and I (.) = |f|2

Depending on this attack, the strength of encryption is evaluated. The approach that is affected less by this attack is considered to provide better encryption.

## IV. PROPOSED RESOURCE SCHEDULING SCHEME

4.1 Simultaneous Compression and Encryption of Optical Images

During transmission, encrypted optical image requires higher bandwidth and rate of transmission gets affected as the encryption process increases its requirements. To overcome this issue, simultaneous encryption and compression of optical images are performed. This is achieved by combining the efficient Direction-Adaptive Discrete Wavelet Transform Compression (DADWTC) with the proposed CKRMDRPE forming CKRMDRPE-DADWTC to simultaneously encrypt and decrypt the optical image.

4.2 CKRMDRPE-DADWTC

In this approach, the CKRMDRPE performs the encryption process as discussed in the previous section while the DADWTC performs the image compression simultaneously.

DADWTC utilizes directional lifting for the compression process. DADWTC initiates a series of processes. The two-dimensional DWT consists of two stages. In the first stage, the 1-D DWT is applied to the image followed by vertical sub-sampling to obtain the low-pass sub-band L, and the high-pass sub-band H. In the second stage, another 1-D DWT is applied to L and H, followed by horizontal sub-sampling to obtain the LL and LH, and the HL and HH sub-band, respectively. It is proved that any two-band bi-orthogonal DWT can be factored into pairs of lifting steps.

Let s={s[l]l ∈ ∏} where s[l] =s[lx,ly] and l=(lx,ly)T, denotes a set of image samples on a 2-D orthogonal sampling grid ∏={(lx,ly)T ∈ $\mathbb{Z}^2$}. To apply 2-D DWT with lifting, initially a transform between the even and odd rows of the image s0 and s1. The results are low-pass sub-band denoted as w0 and high-pass sub-band denoted as w1. Then the 2D- DWT is applied and it is expressed as

$$w_1[l_1] = gH * \left(s[l_1] - P_{l_1}(s_0)\right) \quad \forall l_1 \in \Pi_1$$

$$w_0[l_0] = gL * \left(s[l_0] + g_H^{-1}.U_{l_0}(w_1)\right) \quad \forall l_0 \in \Pi_0$$

Where $P_{l_1}$ is the prediction function and $U_{l_0}$ is the update function, are the functions of the sample values in the input with a scalar output, $gL$ and $gH$ are scaling factors.

Then the directional lifting is applied in which the prediction and the update function are expressed as

$$P_{l_1}(s_0) = \sum_{k=-Kp}^{Kp-1} c_{P,k}\,.\,s\left[l_{1,x}, l_{1,y} - (2k+1)\right]$$

$$U_{l_0}(w_1) = \sum_{k=-KU}^{KU-1} c_{U,k}\,.\,w_1\left[l_{0,x}, l_{0,y} - (2k+1)\right]$$

Where Kp, cP,k, KU and cU,k are determined by the wavelet kernel adopted.

The DADWTC defines direction prediction filters with direction $d = (d_x, d_y)^T$ from which $P_{l_1}(s_0)$ can be selected adaptively

$$P_{l_1}^{d}(s_0) = \sum_{k=-Kp}^{Kp-1} c_{P,k}\,.\,s[l_1 - (2k+1)d]$$

Where d is defined such that

$$l_1 - (2k+1)d \,\epsilon \Pi_0$$

Similarly the update function is expressed as

$$U_{l_0}(w_1) = \sum_{k=-KU}^{KU-1} c_{U,k} \cdot \sum_{\{l_1 l_1-(2k+1)d^*_{l_1}=l_0} w_1[l_1]$$

For the second stage of the DWT further applied to $w_0$and $w_1$, the transform can be applied along directions derived from the set of ds. dy is even and dx is odd and

$$l_{01} - (2k+1)d \in \Pi_{00}, l_{11} - (2k+1)d \in \Pi_{10}, \forall l_{01} \in \Pi_{01}, l_{11} \in \Pi_{11}$$

Despite that with dy>1 in this approach the reference samples are further away from the samples being predicted, experiments indicate that using these samples for prediction is typically more efficient than the interpolated ones in the presence of sharp image features, especially when simple interpolating filters are used. For horizontal image features, i.e., features oriented beyond 45o from the vertical axis, there is no filtering direction closely aligned with the image feature, and, thus, the energy is spread into the high-pass sub-band H rather than contained in L. As a result, for image compression they favour vertical image features and, therefore, are sensitive to image transposition. For image compression, the filtering directions in DADWTC should be chosen to reduce the distortion of the reconstructed image. In order to minimize the overhead, the selection of direction is done in a block-wise manner. For the transform applied to s, the original grid $\prod$ is evenly segmented into Nb non-overlapping blocks, Bb, b=0,1,2,…Nb-1. The direction is chosen by minimizing the Lagrangian cost function

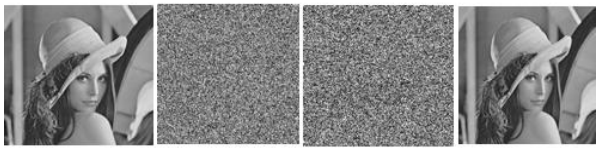
$$d_b^* = \arg min_d \{ \sum_{l_1 \in \Pi_1 \cap B_b} D(gH.(s[l_1] - P_{l_1}^d(s_0))) + \lambda R_b^d \}$$

Where D(.) is a distortion measurement, $\lambda > 0$ is a Lagrangian multiplier, and $R_b^d$ denotes the number of bits spent on signalling the selection $d_b^* = d$.

The cost functions for the transform on and are similarly defined. Although the direction is selected block-wise, filtering in the prediction and update step extends across block boundaries. Therefore, blocking artefacts are not observed in the reconstructed images. To further increase the efficiency of the prediction step, each block may be further partitioned into 2x1, 1x2, 2x2, 4x1, 1x4, 4x2, 2x4, or 4x4 sub-blocks. The best block-partition for each block and the best direction for each sub-block are then selected using the modified cost function, similar to the variable block-size motion compensation in video coding. Then the direction selection is predicted from the selections of the blocks (sub-blocks) in the causal neighbourhood, and the residual is coded with variable-length coding. Then the computational complexity is analyzed for determining the efficiency of the DADWTC. As the Lagrangian cost function is minimized at the block level; hence, the computation required can be neglected. As a result, the computation required, for the DADWTC includes only the KU Multiplications and 2 KU additions. Thus it can provide better compression simultaneously with CKRMDRPE encryption.

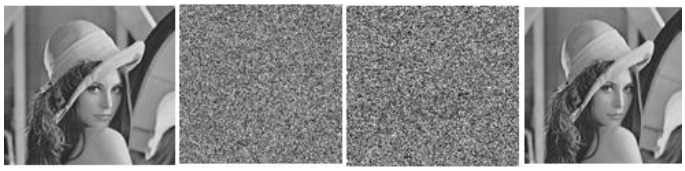
## V. EXPERIMENTAL RESULTS

The optical image encrypted using CBMDRPE and CKRMDRPE are shown below Figure 3 and 4.



(a) (b) (c) (d)

Figure 3. Lena image (a) Original Image (b) CKRMDRPE Encryped image (c) Transmission received image (d) CKRMDRPE Decrypted image



(a) (b) (c) (d)

Figure 4. Lena image (a) Original Image (b) CKRMDRPE-DADWTC Encryped image (c) Transmission received image

(d) CKRMDRPE-DADWTC Decrypted image

On comparing the CKRMDRPE with CKRMDRPE-DADWTC based on performance metrics such as network parameters such as throughput, latency and error rate, the better technique for simultaneous encryption and compression can be found. Figure 3 and Figure 4 shows the encrypted and compressed images using CKRMDRPE and CKRMDRPE-DADWTC, transmitted and decrypted.

### 5.1 Throughput

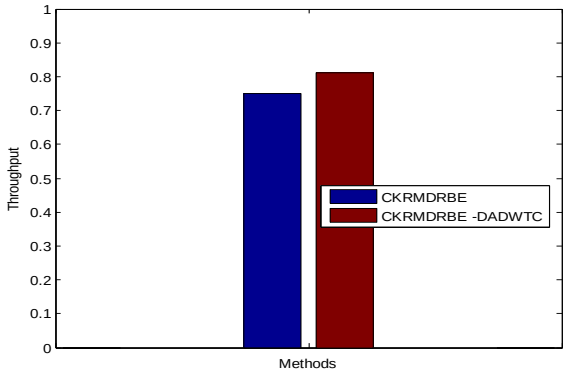



Figure 5 Throughput

Figure 10 shows the comparison of CKRMDRPE and CKRMDRPE-DADWTC in terms of Throughput. CKRMDRPE has 0.75 while CKRMDRPE-DADWTC has 0.8125 which means the CKRMDRPE-DADWTC provides better encryption and compression with increased throughput.

### 5.2 Latency

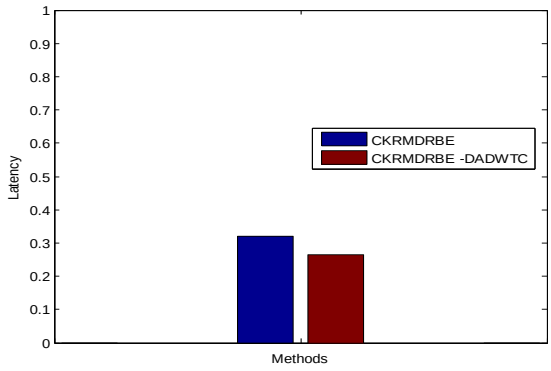



Figure 6 Latency

Figure 6 shows the comparison of CKRMDRPE and CKRMDRPE-DADWTC in terms of latency. CKRMDRPE has 0.3210 while CKRMDRPE-DADWTC has 0.2640 which means the CKRMDRPE-DADWTC provides better encryption and compression with reduced latency.

5.3 Error Rate

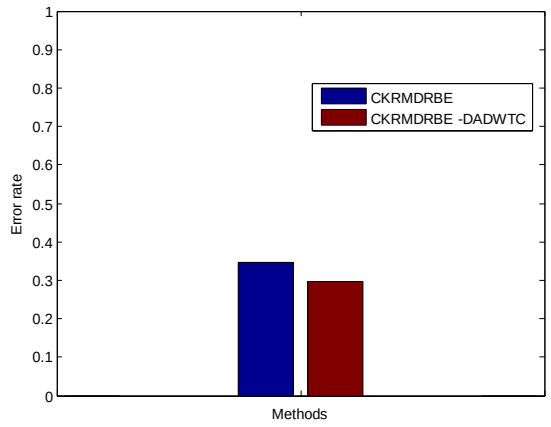



Figure 7 Error rate

Figure 7 shows the comparison of CKRMDRPE and CKRMDRPE-DADWTC in terms of Error rate. CKRMDRPE has 0.3452 while CKRMDRPE-DADWTC has 0.2954 which means the CKRMDRPE-DADWTC provides better encryption and compression with increased error rate.

## VI. CONCLUSION

In this paper, CKRMDRPE is proposed to enhance the security with efficient results. This approach reduces the complexity in computations and increases the speed of mapping by employing bit-wise representation thus enhancing the encryption process. This approach is not affected by the known-plaintext attack ensuring its efficiency by providing better results in terms of maximum deviation, correlation coefficient, mean square error and peak signal-to-noise ratio. . In order to provide simultaneous encryption and compression of optical images DADWTC is implemented with CKRMDRPE to form CKRMDRPE-DADWTC. The performance of the approaches is evaluated in terms of performance metrics and it concludes that the CKRMDRPE provides better encryption while CKRMDRPE-DADWTC is better suited for simultaneous encryption and compression.

## REFERENCES

[1] B. Javidi, A. Sergent, Optical Engineering 36 (3) (1997) 935.
[2] P. Refregier, B. Javidi, Optics Letters 20 (7) (1995) 767.
[3] B. Javidi, E. Ahouzi, Applied Optics 37 (26) (1998) 6247.
[4] N. Towghi, B. Javidi, Z. Luo, Journal of the Optical Society of America A 16 (8) (1999) 1915.
[5] M. Madjarova, M. Kakuta, M. Yamaguchi, N. Ohyama, Optics Letters 22 (21) (1997) 1624.
[6] J.W. Han, C.S. Park, D.H. Ryu, E.S. Kim, Optical Engineering 38 (1999) 47.
[7] E. Tajahuerce, O.Matoba, S.C. Verrall, B. Javidi, Applied Optics 39 (14) (2000) 2313.
[8] Ahmed M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragalla, Yi Mu, Saleh A. Alshebeili, and F. E. Abd El-Samie, “Optical Image Encryption Based on Chaotic BakerMap and Double Random Phase Encoding”, vol 31, August 2013
[9] Zhou, Nanrun, and Taiji Dong. "Optical image encryption scheme based on multiple-parameter random fractional Fourier transform." Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on. Vol. 2. IEEE, 2009.
[10] Lai, Jinhui, Song Liang, and Delong Cui. "A novel image encryption algorithm based on fractional Fourier transform and chaotic system." Multimedia Communications (Mediacom), 2010 International Conference on. IEEE, 2010.
[11] Liu, Zhengjun, et al. "Image encryption based on the random rotation operation in the fractional Fourier transform domains." Optics and Lasers in Engineering 50.10 (2012): 1352-1358.
[12] Liu, Shi, and John T. Sheridan. "Optical encryption by combining image scrambling techniques in fractional Fourier domains." Optics Communications 287 (2013): 73-80

R.Siva Malar received the MCA, M.Phil and M.Sc degrees from Bharathiar University, India in 2006, 2008 and 2009 respectively. She also received her M.E degree from Anna University, India in 2012. Since 2012 she has been working as lecturer in Computer Science department, Jazan University, Kingdom of Saudi Arabia. She is currently doing her Ph.D in Computer Science and Engineering at Jodhpur National University, India. Her research interests are in the areas of resource management and scheduling in the area of Cloud Computing and Image Processing.