A Novel Algorithm of Image Cryptography via Knapsack and Discrete Logarithm Technique

Dr. Adil AL-Rammahi / Kufa University

Department of Mathematics, Faculty of computer science and Mathematics
Najaf, Iraq
adilm.hasan@uokufa.edu.iq

Abstract___*Exploration and expanding of internet usages obliges us to think deeply in secure data via communication. In present time, mutual images via internet spread very fast. It is needed in all electronic dealing, say visa finger print, forensic, military movement, and others. The purpose of this paper is to introduce the method of image cryptography using knapsack KP and discrete logarithm technique DL. In this paper discrete logarithm DL is calculated over cyclic group which deduced from finite Galio field GF(p^n) of order p^n for prime number p. Two steps are achieved in encryption part. The transformation of integer number grey levels of image matrix to binary bit vectors is computed. Then these vectors were enciphered using knapsack crypto method. Finally discrete logarithm is applied for more complicated encryption image. The key of our proposed method was represented as the super increasing bases of knapsack problem and the generator of discrete logarithm field. The statistical measurements of tested images via proposed method are promised well. Many comparisons with related update works were achieved. The compared calculations proved the goodness of proposed algorithm.*

Keywords: Image Cryptography, Knapsack Problem, Discrete Logarithm.

1. INTRODUCTION

Now days, security of mutual digital images via internet became very important. In other hand the images of forensic, finger print, military affairs must saved in secure manner. So these important images must be unread against unauthorized workers. The main purpose of cryptography is to deform the features of image. In other words the original image is deformed or covered in encryption process while the original information is read or recovered only through decrypted process. Encryption or cryptography must occur through mathematical operations. The main idea behind the most present works is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information is presented in an image is due to the correlations among the bits, pixels and blocks of a given arrangement. This perceivable information of encryption can be reduced by decreasing these correlations.

From deep reading of the works of image cryptography, one can classify it with respect to the action of its mathematical operations, named as undervalues cryptography and overvalues cryptography. For undervalues type, the encrypted values varying through allowable integer grey levels interval [0,255]. In this type, a permutation of values is occurred. So the errors or differences between original image and decrypted image are near to vanish, but it encourages the cryptanalyst to detect the origin image. It is occurred in the famous methods of Vernam[1], discrete logarithms via Galio field[2], Ergodic scheme[3], blowfish algorithm[4], XOR operation [5], and others.

For overvalues type, the encrypted values exceeds the allowable grey levels interval [0,255]. In this type, one must work in hard for transforming last form values to pliable values. So the errors or differences between original image and decrypted image are greater than zero. For exceeding this problem, an encrypted image matrix file is calculated and transformed instead of encrypted image. Indeed this type of cryptography is occurred in the methods of calculus[6], singular values decompositions[7], affine transforms[8], chaotic[9], fractal[10], discrete Fourier transform[11], frequency domain transform[12], interpolation[13], approximation[14],and others.

Knapsack cryptography technique transfers conversely between binary bit vectors and integer numbers. The basic concept is concerned on multiplying the bit vector by integer basis vector. So it provides a secure means of exchanging the basis. For related update studies, Krishna algorithm is iterated by the values which are randomly picked from the basin values [15]. Khalifa et al [16] used the combination of RSA (Rivest-Shamir-Adelman) hybrid system and knapsack. Lu and Li [17] used knapsack in the text cryptography. Yamanda et al [18] introduce combination method of knapsack problem and the minimum spanning tree. In Peasah et al algorithm [19], Knapsack is employed in selecting adverts to play on air from a pile of adverts. Roland et al measured the adjustment of encrypted knapsack by the Chebyshev distance [20]. Dean [21] studied the stochastic knapsack problem and its benefit. Bonus, and Boating [22] used knapsack technique in improved shield of drift reduction centre nozzle.

Image cryptography is considered a famous type of applied cryptography. It is demonstrated practically. For update studies of image cryptography, Li and Yuan focused on the encryption of digital image and video with respect to an intrinsic weakness of all existing discrete-cosine-transform (DCT) [23]. Al-Husainy presented mixed method of Boolean operations and rotations [24]. Ogras and Turk [25] introduced digital image encryption scheme using chaotic sequences with a nonlinear fixed functions. Mitra et al [26] proved that the permutation of pixels and blocks are good at producing higher level security compared to bit permutation. Tamilarasi et al [27] encrypted gray scale images by using visual cryptography approach via Halftone algorithm. Sahu et al [28] studied encrypted images using palm algorithm and XOR operation. Younes and Jantan encrypted image using discrete cosine transform[29].

In this paper the composed technique of knapsack and discrete logarithm is used for image cryptography. The grey levels of image matrix are transformed to corresponding bit vectors. Then these vectors are multiplied by the basis of knapsack method and the generator of discrete logarithm field. This basis and the generator are considered as the key of our proposed method. The next procedure of this paper is to present each of knapsack problems and discrete logarithm cryptography mathematically. Then a new algorithm for encrypted and decrypted image is introduced via knapsack problem and discrete logarithm. Finally test images are taken for proving the power of implementation. Statistical measures are calculated for discussing the goodness of our proposed technique. The comparisons of our proposed method with many related updated works were achieved. The calculations of statistical analysis proved that our work was the best. Indeed in this paper discrete logarithm DL is calculated over cyclic group which deduced from finite Galio field.

2. KNAPSACK PROBLEMS

The first usage of knapsack cryptography is used in the area of electronic mail. It may soon be upon us: we must ensure that two properties of the current (Paper mail) system are preserved: (a) messages are private, and (b) messages can be signed [30]. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote each dispenses and computer terminals [31].The following are basic known concepts of knapsack problem named as Merkle-Hellman Algorithm [32].

Merkle-Hellman Algorithm
First part (Encryption)

1) An integer n is fixed as a common system parameter.
2) Choose super increasing sequence $a=(a_1,a_2,...a_n)$ and M such that $M>a_1+a_2+...+a_n$, and $a_i>a_1+a_2+...+a_{i-1}\forall i=1,2,...,n.$
3) Select random integer w, $1\le w\le M-1$, such that the greatest common divisor GCD(W,M)=1.
4) Compute $b=w*a$ mod M.
5) The public key is $b=(b_1,b_2,...b_n)$ and the private key is (M,w,a).
6) The plain bit vector message $x=(x_1,x_2,...x_n)$.
7) The cipher text (y) of (x) is calculated by product operation of (x) and (a) and named as y=dot(x , a).

Second Part (Decryption)

1) Compute $a=w^{-1}*b$ mod M
2) Deduce x from $y=x_1a_1+x_2a_2+...x_na_n$ as the following FUNCTION named as (INF) where the inputs are (y) and (a), while the output is (x).

```
Function x = KPINF (y,a)
    FOR i = n : -1:1
        IF $y\ge a_i$ THEN $x_i=1$ & $y=y-a_i$ ELSE $x_i=0$ END IF
    END FOR.
```

For applying above algorithm on grey levels, TABLE 1 was achieved for basis a=[1,2,4,8,16,32,64,128], w=3, M=337 where x, g, and y, are the plain, plain grey level, and the cipher respectively.

TABLE 1 Knapsack of 8-Bit Vectors

No.	x								g	y
1	1	0	0	0	1	0	0	1	145	326
2	1	1	1	1	1	1	1	1	255	331
3	1	0	1	1	1	1	1	1	253	322
4	1	0	1	1	1	0	1	1	221	217
5	0	0	1	1	1	0	1	1	220	214
6	0	0	1	0	1	0	1	1	212	184
7	0	0	0	0	1	0	1	1	208	166

3. DISCRETE LOGARITHM

The following are basic known definitions and theorems for studying discrete logarithms over Galio field.

Definition 1: If K is a field extenuation of F , the element k ε K is called ***algebraic*** over F if there exist $a_0, a_1, ..., a_n \in F$ not all Zero , such that $a_0 + a_1 k + ... + a_n k^n = 0$ [38,39].

In other words , k is the roots of a non zero polynomial in F[x] (the set of all polynomials where its coefficients belong to F) .

Definition 2: A group (G,+) is called ***cyclic*** if all elements of G can be generated from element g $\in$ G . In this case it is written $G =< q >$ [39].

Theorem1: Let x be algebraic over F and let r(x) be an irreducible polynomial of degree n over F with x as a root. Then $f(x) = F[x]/r(x)$ [39] .

Theorem 2: Let GF*(p^n) be the set of non zero elements in the Galio field GF(p^n). Then (GF*(p^n),.) is a cyclic group of order (p^n – 1) [40] .

Definition 3: A generation g of the cyclic group (GF*(p^n) , .) is called a Primitive element of GF*(p^n) , and for notation by GF*(p^n) = <q> [39,40] .

Example 1: For encoding over GF*(101) = < 2 > ; $y = q^x \mod p$

P	*q*	*P*	*g*	*P*	*q*	*P*	*q*
3	2	7	3,5	13	2,6,7,11	31	3,11,12,13,17
5	2,3	11	2,6,7,8	17	3,5,6,7,10,11,12,14	101	2,3,7,8,11,12

4. IMAGE ENCRYPTION VIA PROPOSED COMPOSED TECHNIQUE OF KNAPSACK PROBLEM AND DISCRETE LOGARITHM

One of the applied cryptography is the digital image cryptography. It is known that the crypto operation must have inverse, but TABLE 1 referred that the cipher (y) exceeds the grey level interval [0,255] via knapsack algorithm. So we use the manner of saved/loaded file through encrypted/decrypted stage. For more complex method against the attacker we study another method where the encrypted data deduce as image. First we transform the data from integer interval [0,255] into real interval [0,25]. Second we transform the grey levels of image matrix to its corresponding bit vectors. Third we use the method of knapsack. Finally we use the method of discrete logarithm. In this proposed composed method, the super increasing basis of knapsack and the generator of discrete logarithm field are used as the key of proposed method. Regarding these notes, one can classify first method as overvalues cryptography while the second as undervalues cryptography. Cryptography algorithms can be classified according to encryption structure into block ciphers and stream ciphers. Each of knapsack technique and discrete logarithm encrypted image is belonging to stream cipher methods. So it has a fast implementation and good running time. Encryption algorithm and decryption algorithm using MATLAB to simulate two new constructed functions. The first function was named as dec2bin8 which it transform the grey level to binary 8- bit vector. The second function was named as kpinf which transforms discrete logarithm to its original binary grey level vector with standard base named as BASE=[128, 64, 32, 16, 8, 4, 2, 1]. For clear our proposed algorithms, we take the grey level x=255, and knapsack basis b=[1 2 4 8 20 40 80 200]. Then in encryption stage, we have,

```
 t=dec2bin8(x)= [1, 1, 1, 1, 1, 1, 1, 1]
y=dot(b,t)=355
```

So we trans 355 as a cipher of 255.

In decryption stage, the descriptor receives y=355. He calculated the following operations to decrypt 355,

z=kpinf(b,y)= [1, 1, 1, 1, 1, 1, 1, 1]
g=dot(z,b_1)=255.

For more clearing, many grey levels encrypted in the following table 2.

TABLE 2 Encryption and Decryption

No.	x	t	y	z	g
1	2	[0,0,0,0,,0,0,1,0]	80	[0,0,0,0,0,0,1,0]	2
2	67	[0,1,0,0,0,0,1,1]	282	[0,1,0,0,0,0,1,1]	282
3	200	[1,1,0,0,1,0,0,0]	23	[1,1,0,0,1,0,0,0]	23
4	90	[0,1,0,1,1,0,1,0]	110	[0,1,0,1,1,0,1,0]	110

For second method we transform grey level to 5-bit vectors. This operation gave as many choices for the increasing basis of knapsack and the generators of discrete logarithm field. For testing the goodness of proposed methods, many images are studied with discussion in next section.

5. STATISTICAL ANALYSIS

Image cryptography must contain two separate stages. The first is named as decryption and the second is referred as decrypted. It is the inverse of encrypted operations. Mathematically, it is known that when small changes occur in encrypted operations tend to large changes of data information, leading to good algorithm. The famous image statistical measurements were determinate by coefficient correlation (COR), peak signal to noise ratio (PSNR), Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). It is noted that PSNR based on the number of vanishing moments. Clearly the attacker may seek to observe variations of the encrypted image in the tiny variations of the plaintext to find the correlation between the plaintext and the encrypted image. If a tiny change in the original image can lead to a great change in the cipher image, then the algorithm can effectively resist these differential attacks. Generally, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) can be used to describe the ability to resist the differential attack. The ideal values of NPCR and UACI are 99.61% and 33.46%, respectively. The four statistical measurements are defined as follows:

$$PSNR = 10 * \log 10(\frac{255*255}{MSE}) \qquad (1)$$

$$ME = \frac{1}{M*N}\sum_{i=1}^{N}\sum_{j=1}^{M}(X(i,j)-Y(i,j))^2 \qquad (2)$$

$$NPCR = \frac{\sum D}{M*N} * 100\% \qquad (3)$$

$$UACI = \frac{1}{M*N}[\sum\frac{|X-Y|}{255}] * 100\% \qquad (4)$$

$$COR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(X(i,j)-E(X))(Y(i,j)-E(Y))}{[\sum_{i=1}^{N}\sum_{j=1}^{M}(X(i,j)-E(X))^2\sum_{i=1}^{N}\sum_{j=1}^{M}\ (Y(i,j)-E(Y))^2]^{\frac{1}{2}}} \qquad (5)$$

$$E(X) = \frac{\sum_{i=1}^{N}\ \sum_{j=1}^{M}(X(i,j)-E(X))}{M*N} \qquad (6)$$

Where D(i,j)=0 if X(i,j)=Y(i,j), otherwise D(i,j)=1. X and Y denote the origin image and its corresponding encryption respectively, each with dimension N*M.

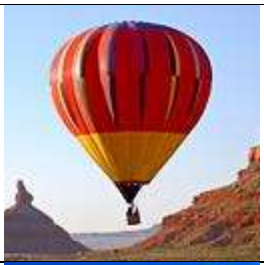
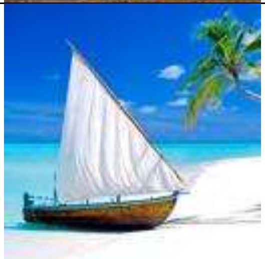
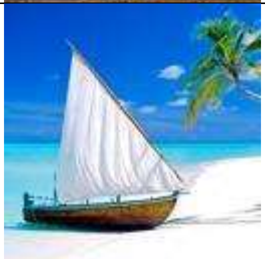
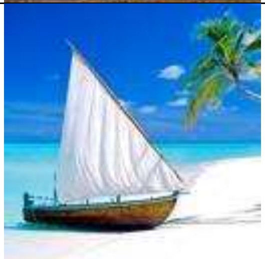
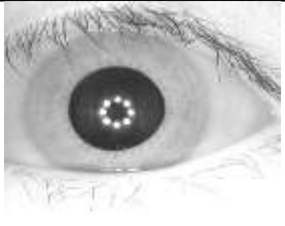
6. IMPLEMENTATION

Two proposed method are introduced for image cryptography. The first method is dealing with knapsack technique only. The second method is represented as a composition of knapsack and discrete logarithm. In the first method we use the knapsack key [1

2 4 8 16 32 64 128] *10 and is denoted by KP. In The second method we use the knapsack key [1 2 3 6 20] and the discrete logarithm key 2 over Z_{101} and is denoted by KPDL. Many images were tested via our two proposed methods. The results proved the feasibility of the proposed algorithms.

Fig. 1 was concerned for test images with its decrypted. In TABLE 3 we notice that the results with respect to second key were better than the first key. So that gave us the justification for using encrypted file matrix image instead of encrypted image. It is noted that the statistical analysis of COR and PSNR with encrypted and decrypted corresponding images were best in second key.

Fig. 1 Test Images

Image	Origin Image	Decrypted with KP	Decrypted with KPDL
Balloon			
Boat			
Bridge			
Eye			
Palm			
Wembley			

Lena			

TABLE 3 PSNR and COR

Image	COR	PSNR
Balloon With KP	0.0619	8.5798
Balloon With KPDL	0.0556	-17.8498
Boat With KP	0.4925	8.5285
Boat With KPDL	0.4556	-17.4937
Bridge With KP	0.3512	8.7467
Bridge With KPDL	0.3169	-16.2539
Eye With KP	0.2510	8.3976
Eye With KPDL	0.2325	-18.6344
Palm With KP	0.0226	8.3847
Palm With KPDL	0.0194	-17.8932
Wembley With KP	0.0930	7.7785
Wembley With KPDL	0.0813	-17.8635
Lena With KP	0.0271	8.1564
Lena With KPDL	0.0224	-17.6892

Our tests are implemented and the corresponding values of NPCR and UACI can be obtained. Thus we can get the average values of NPCR and UACI. The results are shown in TABLE 4.

TABLE 4 NPCR and UACI of Test Images

Image	NPCR	UACI	SIZE
Balloon KP	100	65.9749	128x128
Balloon KPDL	100	50.9699	
Boat KP	81.3660	57.8405	128x128
Boat KPDL	95.6299	36.2108	
Bridge KP	70.2800	47.1758	335x210
Bridge KPDL	87.5537	12.5069	
Eye KP	100	72.6937	320x480
Eye KPDL	100	62.5065	
Palm KP	99.7112	65.6730	273x293
Palm KPDL	99.9150	25.5059	
Wembley KP	97.4355	64.9072	580x390
Wembley KPDL	99.4545	21.9736	
Lena KP	100	63.7588	256x256
Lena KPDL	100	53.4881	

7. COMPARISON WITH RELATED WORKS

The calculations of NPCR and UACI of our work proved the goodness of the algorithm. Those calculations are encouraged, but it is not enough for its dependency . For sake of checking the power full of proposed algorithm, many updated related works were studied, then compared with. For relevancy with update related work, a comparison with the work of Ghode et al [33] is studied. Indeed they used the concept of sieving shuffling transformation algorithm to image cryptography. They published their results without decryption images. Their PSNR for Lena image(of size 128x128) was calculated as 42.580, while in our proposed method was 67.5213.

A good encrypted grayscale image algorithm was introduced by Tong et al [34]by using the chaotic sequences which generated by Runge-Kutta method. Two grayscale tested images were published in [35]. The comparison between our proposed algorithm and tong et al proved that our algorithm was the best. The two images with corresponding decryption and encryption were placed in FIG. 2 while the statistical results were calculated and noted in TABLE 5.

Fig. 2 Comparison with Tong et al[34]

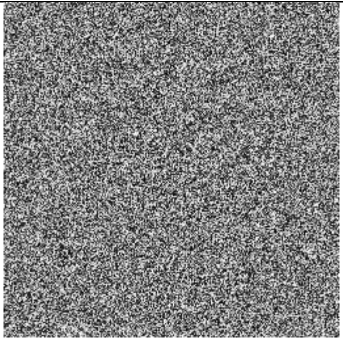
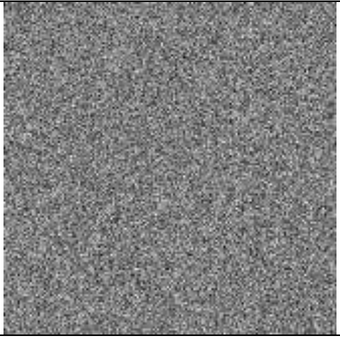
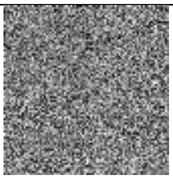
Image	Origin	Encrypted [34]	Decrypted (Proposed)
Lena			
Jokul			

TABLE 5 Comparison with Tong et al[34]

Image	NPCR	UACI
Lena [34]	99.4900	33.3200
Lena KP	99.9985	65.6692
Lena KPDL	100.0000	53.4881
Jokul [34]	99.4400	33.2800
Jokul KP	99.8940	65.5666
Jokul KPDL	99.9105	30.9180

Sivakumar and Venkatesan [35] introduced a good study of image cryptography using scan pattern, circular shift, and bitwise XOR transposition method. They presented a good survey of related studies with comparison. They proved that their algorithm was the best among many algorithms. They taken two images in details for encrypted and decrypted stages. Fig 3. was concerned for presenting those images. The comparisons of proposed method with the work of Sivakumar and Venkatesan were put in Table 6.it is noted that our proposed method is the best.

Fig. 3 Comparison with Sivakumar /Venkatesan [35]

Image	Origin	Encrypted [35]	Decrypted [35]	Decrypted (Proposed)
Lena				

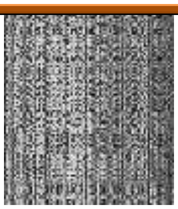
Baboon				

TABLE 6 Comparison with Sivakumar /Venkatesan [35]

Image	NPCR	UACI
Lena [35]	99.4990	33.4200
Lena KP	100	65.2734
Lena KPDL	100	53.4881
Baboon [35]	99.5500	33.4800
Baboon KP	99.8540	66.2804
Baboon KPDL	99.9750	28.3703

Abd El-Wahed et al [36] studied the encrypted method of permutation and diffusion of pixel value. Their paper was not contained any image and the NPCR was up to 87. So One can say that our proposed method was the best.

Rad et al [37] encrypted image using the composed method of scan pattern and XOR operation. Their test images were presented in details. Their related statistical analysis proved the goodness of the work. A comparison of our proposed work with [37] is achieved as showing in TABLE 7.

TABLE 7 Comparison with Rad et al[37]

Image	NPCR	UACI
Lena [37]	99.6135	33.6548
Lena KP	100	65.2734
Lena KPDL	100	53.4881
Barbara [37]	99.6669	33.6548
Barbara KP	100	65.1640
Barbara KPDL	100	31.6948
Camera man [37]	99.6529	33.6015
Camera man KP	99.6672	64.7401
Camera man KPDL	99.8563	37.5509
Pepper [37]	99.5987	33.6001
Pepper KP	99.2550	64.9876
Pepper KPDL	99.7133	28.5139

From the calculations which appears in above table, it is noted that NPCR tend to ideal in both algorithms. And UACI of proposed work is better than [37].

8. CONCLUSIONS

Till now many image cryptographic algorithms have been achieved. Every algorithm is simply based on math concepts, discrete frequency, permutation, diffusion, partitions, special linear transformations, chaotic function, etc. But this proposed cryptographic algorithm is based on flexible method of knapsack problem and discrete logarithm. In this algorithm the basis of knapsack is deal as the key of our algorithm. That gave us many choices of constructing the key where the data are encrypted in color matrix file via MATLAB. Table 3 tell us that the complexity deduced from choosing the key with large and diffusion numbers. When we observe the Performance statistical analysis, always the COR, PSNR, NPCR, and UACI are tending to ideal states. All those statistical analysis are proved the goodness of proposed algorithm. It is noted that all comparisons with related updated works showed that our proposed algorithm is the best. Our algorithm was compared successfully with famous hard worked researchers. And the good results encourage the all for applying and improving our algorithm of knapsack and discrete logarithm. Two algorithms were studied and compared with related updated methods. The first algorithm is concerned for knapsack only while the second algorithm is represented as a composed idea of knapsack and discrete logarithm over Galio field. Another advantage is that our algorithm deals with color and grayscale images.

9. REFERENCES

[1] S. Dey (2012). An Image Encryption Method: Sd-Advanced Image Encryption Standard: Sd-Aies**,** International Journal Of Cyber-Security And Digital Forensics. 1(2), Pp. 82-88.

[2] Al-Rammahi, (2014). Image Encryption Via Discrete Logarithm Over Galio Field , To Be Published At Journal Of Computer Mathematics, Taylor And Francis Publisher.

[3] M. Brin, and G. stuck (2002). Introduction to Dynamical Systems, Cambridge university press, 1st e.

[4] I. Landge, , B. Contractor, A. Patel, and R. Choudhary, (2012). Image encryption and decryption using **blowfish** algorithm, World Journal of Science and Technology, 2(3),pp.151-156.

[5] J. Shah and V. Saxena, (2011). Performance Study On Image Encryption Schemes, Ijcsi International Journal Of Computer Science Issues, Vol. 8, Issue 4, No 1, Pp. 349-355,July.

[6] A. AL-Rammahi, (2014). Encryption Image Using Small Order Linear Systems and Repeated Modular Numbers, To be published at The International Conference of Applied and Engineering Mathematics, World Congress on Engineering, International Association of Engineers, pp. July.

[7] N. AL-Ebadi, A. AL-Rammahi, And M. AL-Kufi, (2014). Image Encryption Based on Singular Value Decomposition, Journal of Computer Science 10 (7), pp. 1222-1230.

[8] M. A. Shreef and H. K. Hoomod, (2013). Image Encryption Using Lagrange-Least Squares Interpolation**,** International Journal of Advanced Computer Science and Information Technology, Vol. 2, No. 4, Pp. 35-55.

[9] H. Gao,Y. Zhang, S . Liang, and D. Li, (2006). A New Chaotic Image Encryption Algorithm, Chaos, Solitons and Fractals 29, pp. 393–399.

[10] **P.** Sharma, D. Mishra, A. Agarwalefficient, (20124). Image Encryption And Decryption Using Discrete Wavelet Transform And Fractional Fourier Transform**,**Acm Journal, Digital Library Publisher, Pages 153-157.

[11] P. Bamotra And P. Dwivedi, (2012). Secure Transmission of Grayscale Images Using Discrete Fourier Transform, International Journal Of Sot Computing And Engineering ,Pp. 206-209.

[12] M. A. Hassan, (2011). Image Encryption Using Differential Evolution Approach In Frequency Domain ,Signal & Image Processing, Vol.2, No.1, March.

[13] L. Luo , B. hina, Z. Chen, M. Chen, X. Zeng, (2010). Reversible image watermarking using interpolation technique, information forensic and security, IEEE, Volume 5 , Issue1,PP.I87-193.

[14] M. Alkhasaawna and S. Aviyente, (2008). Image encryption scheme based on using least squares approximation technique, IEEE international conference on Electro/Information Technology, volume 1, issue 1, pp.108-111.

[15] A.V.N. Krishna**,** (2012.). An Improvised ECC Mechanism with Probabilistic Approach, Information Security Journal: A Global Perspective ,vol 21, no.1, pp. 28-35.

[16] S.M. Kallpha, J.W. Abdul Sada & H. A. Hussain, (2012). New Public-Key cryptosystem , International Journal Of Systems Science,Vol.1, No.1,Pp. 205-215.

[17] Y. Lu & J. Li, (2013). New forward-secure public-key encryption without random oracles, International Journal of Computer Mathematics, Vol. 90, Issue 12, pp. 2603-2613.

[18] T. Yamada, K. Watanabe And S. Kataoka, (2013). Algorithms To Solve The Knapsack Constrained Maximum Spanning Tree Problem, International Journal Of Computer Mathematics, Taylor & Francis Group Publisher, Vol. 82, No. 1, January 2005, 23–34.

[19] O.K. Peasah, S. K. Amponsah and D. Asamoah, (2011). Knapsack problem: A case study of garden city radio (GCR), Kumasi, Ghana,African Journal of Mathematics and Computer Science Research , Academic Journals Vol. 4(4), pp. 170 -176, April.

[20] J. Roland, Y. Smet, and J. Fegueira, (2011). The Inverse Multi-Objective {0, 1}-Knapsack Problem Under The Chebyshev Distance, Technical Report Number, Pp. 1-9.

[21] B. C. Dean, M. X. Goemans, J. Vondrak, (2008). Approximating the Stochastic Knapsack Problem: The Benefit of Adaptivity, Mathematics Of Operations Research, Inform Publisher Vol. 33, No. 4, November, Pp. 945–964.

[22] P. O. Bonsu, and M. A. Boateng, (2013). Improved shield for knapsack sprayers, Agricultural Science Research Journals, International Research Journals publisher, Vol. 3(3), pp. 93-96, March.

[23] W. Li And Y. Yuan, (2007). A Leak And its Remedy In Jpeg Image Encryption, International Journal Of Computer Mathematics, Taylor & Francis Publisher, Volume 84, Issue 9, Pp. 1367-1378.

[24] M. A. F. Al-Husainy, (2012). A Novel Encryption Method for Image Security**,** International Journal of Security and Its Applications, Vol. 6, No. 1, January.

[25] H. Ogras, M. Turk, “ Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function”, World Academy of Science, Engineering and Technology, Vol:67 ,pp. 7-21, 2012.

[26] A. Mitra, Y. V. S. Rao and S. R. M. Prasanna, (2008). A New Image Encryption Approach using Combinational Permutation Techniques, World Academy of Science, Engineering and Technology, Vol:14, pp. 02-27.

[27] W. Diffie, M.E. Hellman , (1976). New Directions in Cryptography, IEEE Transactions On Information Theory, Vol. 22, N. 6, Pp. 644-654.

[28] A. M. Odlyzko, (1986). New Analytic Algorithms In Number Theory, Proceedings International Congress of Mathematicians, American Math. Soc Pp. 466-475.

[29] M. Younes and A. Jantan, (2008).Image Encryption Using Block-Based Transformation Algorithm, IAENG International Journal of Computer Science, 35:1, pp. 407-415.

[30] R. Merkle, and M. Hellman, (1978). Hiding Information And Signatures in Trapdoor Knapsacks, IEEE Transaction on Inform. IT-24, 5,Sept., 525-530.

[31] J. Tamilarasi, V. Vanitha, T. Renuka, (2014). Improving Image Quality In Extended Visual, Cryptography For Halftone Images With No Pixel Expansion, International Journal Of Scientific & Technology Research Volume 3, Issue 4, April, Pp. 126-131.

[32] A. Sahu, Y. Bahendwar, S. Verma, P. Verma, P. Verma, (2012). Proposed Method Of Cryptographic Key Generation For Securing Digital Image, International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 2, Issue 10, October, Pp. 285-291.

[33] P.s. Ghode, p. Patil, v. Nayyar , (20143). A Keyless approach to Lossless Image Encryption, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May, pp. 1459-1467.

[34] X. Tong, Y. Liu, M. Zhang, H. Xu, and Z. Wang, (2015). An Image Encryption Scheme Based on Hyperchaotic, Rabinovich and Exponential Chaos Maps, Entropy, 17, pp. 181-196.

[35] T. Sivakumar and R. Venkatesan, (2014). A Novel Approach for Image Encryption using Dynamic SCAN Pattern, IAENG International Journal of Computer Science, 41:2, May, pp. 1-11.

[36] M. Abd El-Wahed, S. Mesbah, and A. Shoukry, (2008). Efficiency and Security of Some Image Efficiency and Security of Some Image, Proceedings of the World Congress on Engineering , WCE London, U.K., July 2 - 4, , Vol. I, pp. 1-4.

[37] R. Rad, A. Attar, and R. Atani, (2013). A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.6, No.5, pp.275-290.

Author

Adil ALRammahie, He obtained a bachelor's degree in mathematics from the College of Science, Al-Mustansiriya University in 1989, and obtained a master's degree in stability of large systems from University of Technology in 1996. He also obtained a Ph.D degree in the specialty of fractal numerical analysis in 2005, as well as a professorship title in 2014 from the University of Kufa, and he has been one of its professors for thirty years. During which he held the positions of head of scientific departments and administrative assistant, as well as scientific and head of the scientific and promotions committee. He has several research participations in the Los Angeles Conferences on Medical Images, the Geneva Conference on Communication Networks, and the Paris Conference on Science and Engineering. He has several research papers published in international journals, namely fractal geometry, numerical analysis, differential and integral equations, and cryptography.

.