Proposal Cryptography Algorithm Based On Bit Plane Image Slicing Using Wavelet Transform

***Assist. Prof. Dr. Maisa'a Abid Ali Khodher** ****Assist. Lect. Alyaa Hasan Zwiad**
Computer Science Department
University of Technology
Baghdad, Iraq
[***110044, **110134]@uotechnology.edu.iq**

Abstract:

This paper, a proposed new algorithm it has using image bit plane slicing (BPS), image Haar wavelet transform (HWT), and secure force (SF). It can be provided to any picture which can be sent across the network or transmitted using any way. The proposed algorithm is divided into three parts. *The first part* is composed original image for eight image in bit plane slicing to eight 1-bit in each pixels. *In the second* part which is compressing image in Haar wavelet transform (HWT), in each eight 1-bit image, for reducing size of image. *The third part* which is the cryptography of eight 1-bit image by (SF) method after wavelet transform. Get efficient and powerful method in these three parts. It has cryptography of image to be sent across internet network without visual sensitivity attackers. The form and information in image without detect by attackers through sent to receiver.

Keyword: cryptography, Bit Plane, Wavelet Transform, Secure Force, Image processing.

اقتراح خوارزمية تشفير بالاعتماد على بت طائرة لتقطيع الصورة باستخدام تحويل المويجات

أ.م.د. ميساء عبد علي خضر م.م. علياء حسن زويد

قسم علوم الحاسوب

الجامعة التكنولوجية

بغداد، العراق

الملخص

هذا البحث تم اقتراح خوارزمية جديدة باستخدام طريقة البت الطائرة BPS ، وطريقة تحويل المويجات HWT ، وطرقة القوة الامنة SF في هذا البحث ممكن ارسال أي صورة عبر شبكات الانترنيت وبأي طريقة. وتنقسم هذه الخوارزمية الى ثلاثة اجزاء: الجزء الاول يمكن استخدام طريقة البت الطائرة بت واحدة لكل نقطة في الصورة وتقسم الصورة الاصلية الى ثمانية صور. الجزء الثاني هو ضغط الصور الثمانية بت بعد تقسيمها وذلك لتقليص حجم الصورة باستخدام طريقة التحويل الموجي. الجزء الثالث هو تشفير الصور الثمانية واحد بت بعد التحويل المويجات بواسطة طريقة FS. تم الحصول على طريقة كفؤة وقوية باستخدام هذه الاجزاء الثلاثة. وان تشفير هذه الصورة وارسالها عبر شبكات الانترنيت لايمكن ان يتحسسها ويراها المهاجم، وكذلك البيانات والمعلومات في الصورة لايمكن ان يكتشفها المهاجم من خلال ارسالها الى المستلم.

مفاتيح البحث: التشفير، البت الطائرة، تحويل المويجات، القوة الآمنة، المعالجة الصورية.

1- Introduction:

M
odern improve area of communicate and computer networks grow the defying
for network safety, scalability and precision [1].

One of the greatest used steps in the process of decreasing images to data is dividing: segmentation of the image into regions that hopefully match structural units in the place or differentiate objects of benefit. Segmentation is frequently described by symmetric to visional operation as a foreground/ background differentiation, implying that the chosen procedure focuses on one type of characteristics and discards the rest [2].

In images form, textile, and other low-level image which distinguishes color data one significant characteristic which has successfully used in many image treatment applications such as like "object recognition, image matching, image enhancement, content-based image retrieval, computer vision, color image compression", etc. "Color science still remains defying field of study in the computer vision and digital image processing community today" [3].

2- Bit Plane Slicing (BPS)

The gray scale which is made to overall image manifestation, by specified bits might be wanted. The bit plane slicing assumes that each pixel in an image is illustrated by 8- bits."Imaging that the image is composed of eight 1-bit planes, ranging from bit plane 0 for the least significant bit to bit plane 7 for the most significant bit" [4]. In 8-bit bytes

, plane 0 comprise all the lowest arrangement bits in the bytes including the pixels in the image and plane 7 comprise all the high arrangement bits. in Figure (1), and Figure (2) shown example of bit plane slicing [5].

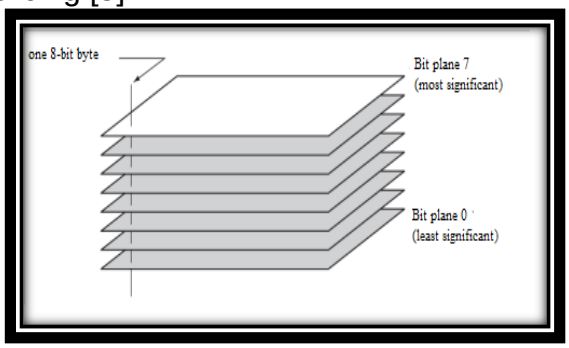


Figure (1). The Bit Plane Slicing [4].

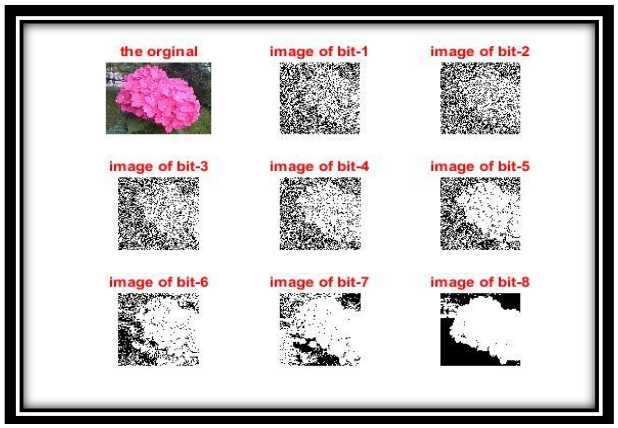


Figure (2): Example of The Bit Plane Slicing [5].

3- Haar Wavelet Transform (HWT)

Haar Transform is memory efficiency, properly inverse without the edge effect, it is fast and easy [6], [7]. The Haar Wavelet Transform (HWT) is one of the easy and basic transformation from "the space domain to a local frequency domain". "HWT decomposes each signal into two components, one is called average (approximation) or trend and the other is known as difference (detail) or fluctuation" [6], [7]. "A precise formula for the values of first average subsignal" , $A^1 = (A_1, A_2, \ldots A_{N/2})$, at one level for a signal of length *N i.e.* $F = (F_1, F_2, \ldots F_N)$ is

$$A_n = \frac{F2n-1+F2n}{\sqrt{2}} ,$$

$$n = 1, 2, 3, \ldots . . N/2, \ldots (1)$$

And the first detail subsignal , $D^1 = (D_1, D_2, \ldots\ldots D_{N/2})$, at the same level is given as

$$A_n = \frac{F2n-1-F2n}{\sqrt{2}} ,$$

$$n = 1, 2, 3, \ldots . . N/2, \ldots (2)$$

in order to given an idea of its implementation in image compression [6]. The LL is the original image in this level, shown in Figure (3).

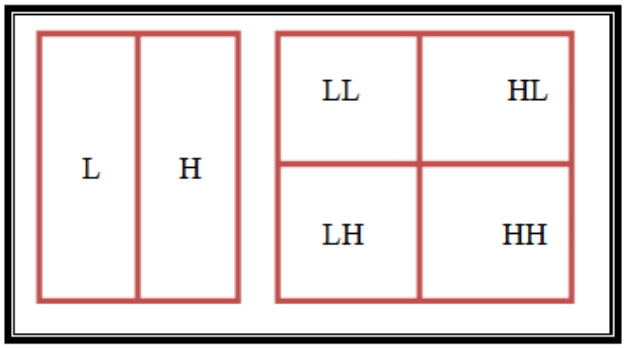


Figure (3): The Haar Wavelet Transform.

4-Secure Force Algorithm (SF)

The Secure Force algorithm is built on an architecture where the operations of encipher and decipher are almost similar, which reduces the code volume to a large extent. The styling of SF algorithm prepare low-complexity architecture for implementation in WSN. To enhance, the power efficiency, the encryption operation consists of only five encipher cycles. A lower number of encipher cycle will lead to less energy consuming. In order to develop the security, each encipher cycle comprises six easy arithmetical operations operating on only 4 bit data "(designed to be compatible with 8-bit computing devices for WSNs)" [1], [8].

This is to make a sufficient amount of confusion and diffusion of information to face, different kinds of attackers. The key extension, operation, which includes complex arithmetical operations "(multiplication, permutation, transposition and rotation)" to create keys for the encipher process, is executed at the decoder [1], [8].

5-Proposed Algorithm

A new algorithm is proposed using cryptography image by secure forces method. It uses three steps. In *the first step* bit plane

slicing is applied to compose original color image to eight 1 bit plane in each pixel in image, *the second step* Haar Wavelet Transform (HWT) is applied in level 2 and level 3 in each 1 bit plane from 0 bit plane to 7 bit plane, and *the third step* applies secure force around of multiplication, permutation, transposition, and rotation in each image after Haar Wavelet Transform (HWT).In
this algorithm SF obtains the cryptography image without detecting sensitive attacks through transmitting internet network.

- **First Step:** This step uses color image RGB to convert gray scale image because image is composed of eight 1 bit plane slicing in each pixel. Each pixel is
represented in color image of RGB value
to binary values, and is composed of 0 bit
plane in LSB to 7 bit plane in MSB.

For example*:* Color image values to
binary values shown in Figure (4).

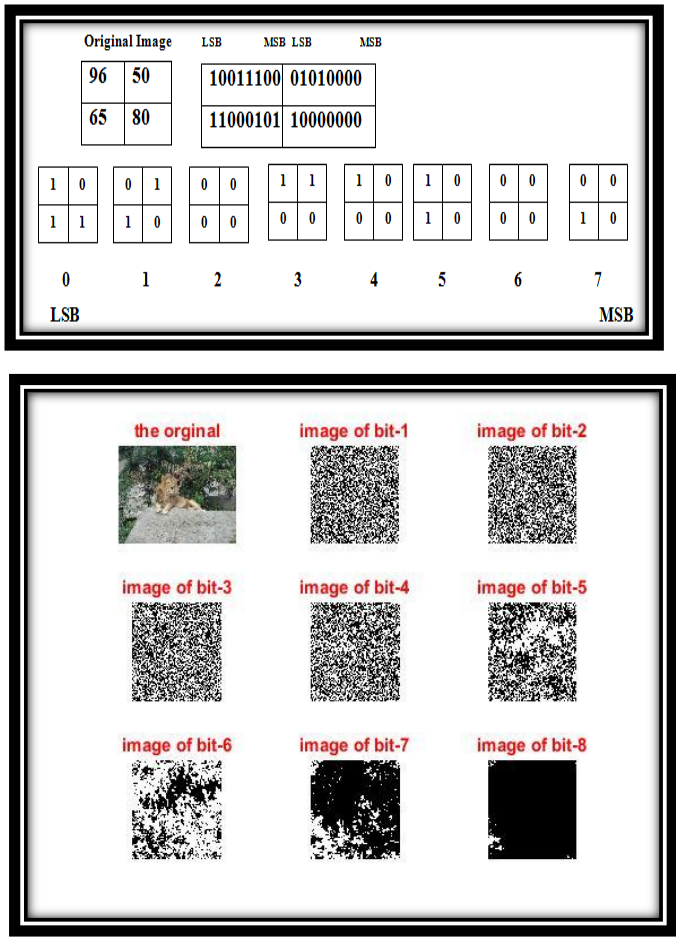


Figure (4): Color Image of Binary Image In Bit Plane.

- **Second Step*:*** This step uses Haar Wavelet Transform (HWT) for each eight images from LSB to MSB in bit plane slicing, and each image compresses one bit to seven bit by HWT in two levels.

Level two compresses image in 16 and level three compresses image in 32.

- **Third Step*:*** This step uses secure force algorithm (SF) for encrypting image after wavelet transform for image distortion to prohibit a known that image, and prohibit visual sensitivity attackers. This algorithm uses four complex operation by encrypted image wavelet.
  - The four complex operations are: Multiplication, Permutation, Transposition, and Rotation and key expansion.

  Step 1: Key = [K1, K2, K3, K4, K5]
  Step 2: Hex_Key = 133457799bbcdff1
  Step 3: Bin_Key = Hex2Bin(Hex_Key)
  Step 4:[K1, K2, K3, K4, K5]=
  SF_Key_Gen (Bin_Key)

  1- First for matrix of 16 bit int4*4 each K1 (1:16); K2 (17:32); K3 (33:48); K4 (49:64);
  2- Second for generating matrix of each 16 bit int4*4
  3- Shifting key [K1, K2, K3, K4] and permutation
  4- Transposition [K1, K2, K3, K4]
  5- Rotation [K1, K2, K3, K4]

  Encryption:

  Step1: For first round :Perform xnor operation in first 16 bits with K1
  Step2: For second round : Perform xnor operation with K2
  Step3: For third round : Perform xnor operation in the first 16 bits with K3
  Step4: For fourth round : Perform xnor operation with K4
  Step5: For fifth round : Perform xnor operation with K5

  Decryption:

  Step1: For first round : Perform xnor operation with K5
  Step2: second round : Perform xnor operation with K4
  Step3: For third round :Swiping Block: performing xnor operation of first 16 bits with K3
  Step4: For fourth round : Perform xnor operation with K2

Step5: For fifth round : Swiping Block:
performing xnor operation of first 16 bits with K1

The flowchart of algorithm of encrypted image using SF, is shown step by step in Figure (4).

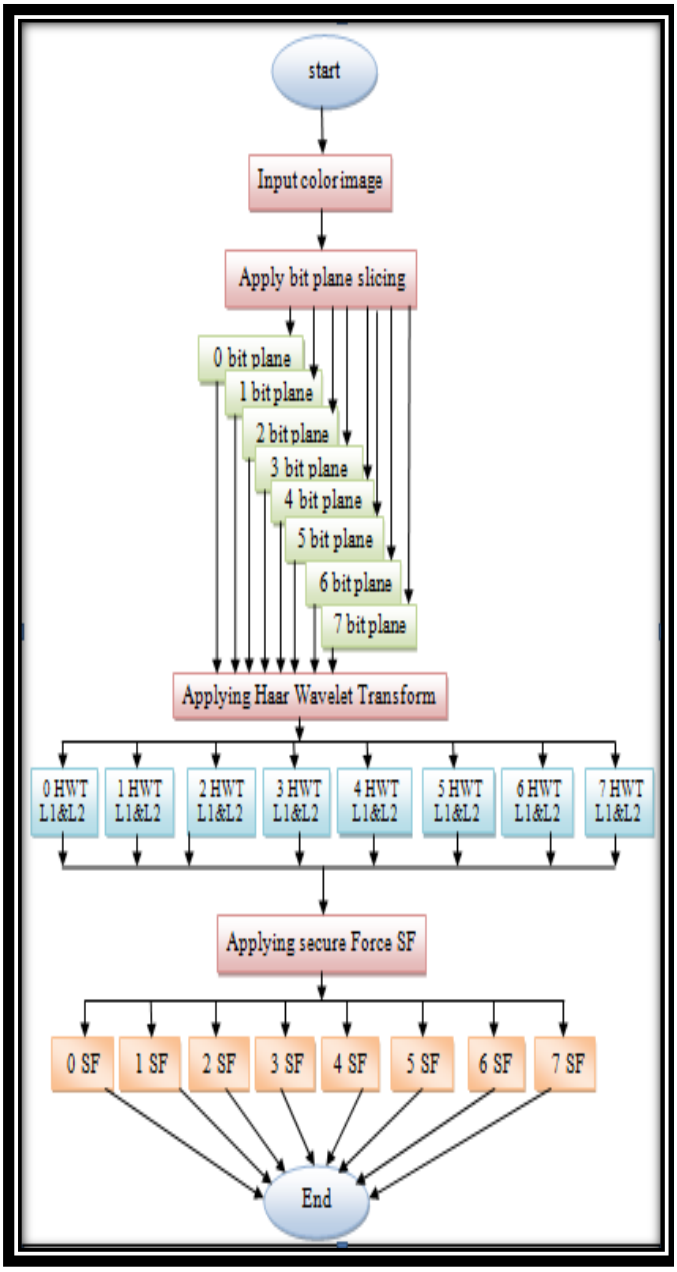


Figure (4): The Flowchart of Algorithm of encrypted image.

A- *Encrypted Process:*

Encrypted Image Algorithm:

Process:

Input: Original Image, Bit Plane Slicing, Wavelet Transform , SF.

Output: Encryption Image.

Initial:

A= Load Original Image.

B= Execute Bit Plane Slicing.

C= Execute Haar Wavelet Transform.

D= Execute Secure Force.

E= Encryption Image.

Step1: Compose Original Image For 0 Bit Plane To & Bit Plane In B.

Step2: Compress Image of 0 Bit Plane To 7 Bit Plane In Wavelet Transform in L2 In C.

Step 3: Compressed Image of 0 Bit Plane To 7 Bit Plane In Wavelet Transform in L3 In C.

Step 4: Apply Secure Force In Eight 1 Bit Plane Image In D.

Step 5: Apply Secure Force In Multiplication.

Step 6: Apply Secure Force In Permutation.

Step 7: Apply Secure Force In Transposition.

Step 8: Apply Secure Force In Rotation.

Step 9: Result (Put The result of Encrypted Image In E).

B- Decrypted Process:

Decrypted Image Algorithm:

Process:
Input: Encrypted Image
Output: Original Image
Initial:
A = Load Encryption Image.
B = Execute Inverse Secure Force.
C = Execute Inverse Haar Wavelet Transform.
D = Execute Sum of Bit Plane Slicing.
E = Original Image.
Step 1: Apply Inverse Secure Force Rotation.
Step 2: Apply Inverse Secure Force Transposition.
Step 3: Apply Inverse Secure Force Permutation.
Step 4: Apply Inverse Secure Force multiplication.
Step 5: Apply Inverse Secure Force in Eight 1 Bit Plane In B
Step 6: Apply Inverse Wavelet Transform in L3 image of 0 Bit Plane to 7 Bit Plane In C.
Step 7: Apply Inverse Wavelet Transform in L2 image of 0 Bit Plane to 7 Bit Plane In C.
Step 8: Summation 0 Bit Plan To 7 Bit Plane In D.
Step 9: Result (Put The result of Original Image In E).

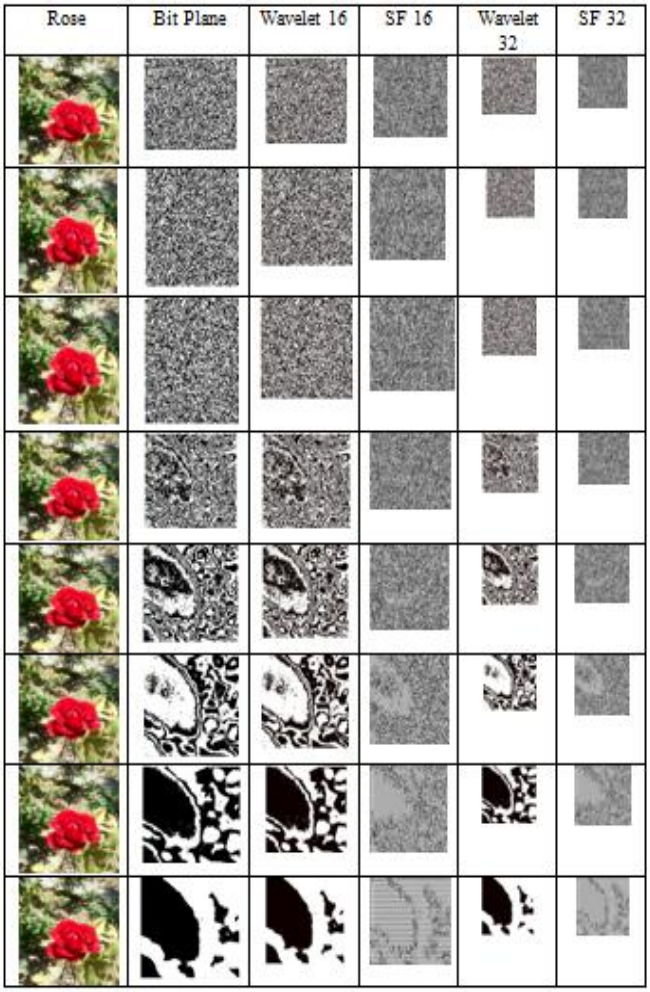
6- Test of Result

The implementation of system in bit plane, wavelet in 16 , 32, and SF in 16, 32, is shown in Table (1) and Table (2). The system is powerful in image

security, and without sensitively by attackers.

Table (1): Implementation System of Cryptography.

Table (2): Implementation System of Cryptography.



• Table (3) and Table (4) indicate distortion measures in image processing in PSNR, RMAE, MSE, correlation.

Table (3): Distortion Measures in Level 2 and Level 3

Distortion Measures	PSNR	RMAE	MSE	Correlation
Original Girl	0.9486	157.7714	24891.8223	5.23866
Bit plane1	1.0218	152.5584	2327.0795	3.62830
Bit plane2	0.6412	182.6103	33346.5195	1188.8324
Bit plane3	0.64122	182.6103	33346.5195	1188.83246
Bit plane4	0.56195	189.8882	36057.5481	1472.18835
Bit plane5	1.30743	134.3635	18053.5464	2173.81838
Bit plane6	0.2824	218.9995	47960.7603	3163.7268
Bit plane7	1.7351	112.3842	12630.2156	11268.9547
Bit plane8	1.8126	108.9554	11871.2687	12536.5574
Wavelet16 1	0.6820	179.0078	32043.7794	74.54300
Wavelet16 2	0.6600	180.9415	32739.8342	103.7429
Wavelet16 3	0.6600	180.9415	32739.8342	103.7429
Wavelet16 4	0.5765	188.516	35538.27561	240.54175
Wavelet16 5	1.3238	133.4115	17798.62521	560.97829
Wavelet16 6	0.2975	217.2696	47206.0836	1400.3890
Wavelet16 7	1.7986	109.5643	12004.3427	8738.6654
Wavelet16 8	1.8765	106.2427	11287.5132	9318.66437
Wavelet32 1	0.6820	179.0078	32043.7794	74.543006
Wavelet32 2	0.6600	180.9415	32739.8342	103.74292
Wavelet32 3	0.6600	180.9415	32739.8342	103.7429
Wavelet32 4	0.5765	188.516	35538.2756	240.54175
Wavelet32 5	1.3238	133.4115	177798.6252	560.97829
Wavelet32 6	0.2975	217.2696	47206.0836	1400.3890
Wavelet32 7	1.7986	109.5643	12004.3427	8738.6654
Wavelet32 8	1.8765	106.2427	11287.5132	9318.6643
SF16 1	1.03721	151.4909	22949.4875	0.66667
SF16 2	1.0005	154.0464	23730.2825	0.58442
SF16 3	1,0005	154.0464	23730.2825	0.584422
SF16 4	0.96183	156.8124	24590.1330	0.59743
SF16 5	0.96183	156.8124	24590.13308	0.597438
SF16 6	0.85820	164.5633	27081.0807	0.87678
SF16 7	0.78269	170.5512	29087.70155	6.90273
SF16 8	0.7820	170.6046	29105.92029	7.91570
SF32 1	1.03721	151.4909	22949.48755	0.66667
SF32 2	1.00056	154.0464	23730.28252	0.584422
SF32 3	1.00056	154.0464	23730.28252	0.584422
SF32 4	0.9618	156.8124	24590.13308	0.5974385
SF32 5	0.9042	161.0526	25937.9272	0.7154788
SF32 6	0.85820	164.5633	27081.08076	0.87678
SF32 7	0.78269	170.5512	29087.70155	6.902730
SF32 8	0.78203	170.6046	29105.92029	7.9157052

Table (4): Distortion Measures in Level 2 and 3.

Distortion Measures	PSNR	RMAE	MSE	Correlation
Original Rose	0.77948	170.812	29176.7472	3.466496
Bit plane1	0.68435	178.8116	31973.5894	1224.8115
Bit plane2	0.71541	176.1437	31026.6167	1156.3688
Bit plane3	0.6914	178.1998	31755.18554	1153.17958
Bit plane4	0.7123	176.4018	31117.59932	816.737743
Bit plane5	0.6839	178.8445	31985.34013	681.167135
Bit plane6	0.63060	183.563	33695.39350	844.09849
Bit plane7	0.75746	172.6122	29794.97999	1758.07779
Bit plane8	0.48970	196.8756	38760.00355	2575.94698
Wavelet16 1	0.70133	177.3461	31451.63125	82.59454
Wavelet16 2	0.73164	174.7712	30544.9849	78.523799
Wavelet16 3	0.70632	176.9192	31300.41235	76.76802457
Wavelet16 4	0.72371	175.44	30779.20947	66.05177955
Wavelet16 5	0.69761	177.666	31565.21886	68.04032299
Wavelet16 6	0.64268	182.48	33298.9636	179.593001
Wavelet16 7	0.78604	170.2791	28994.97900	527.49649
Wavelet16 8	0.51021	194.8565	37969.05664	13391.1390
Wavelet32 1	0.71338	177.3461	31451.6312	82.594521
Wavelet32 2	0.73164	174.7712	30544.98495	78.523799
Wavelet32 3	0.70632	176.9192	31300.41235	76.768024
Wavelet32 4	0.72371	175.44	30779.20947	66.051779
Wavelet32 5	0.69761	177.666	31565.21886	68.0403229
Wavelet32 6	0.64268	182.48	33.298.96360	179.59300
Wavelet32 7	0.79604	170.2791	28994.97900	527.49649
Wavelet32 8	0.51021	194.8565	37969.05664	13391.1390
SF16 1	1.09412	147.6397	21797.48757	0.676041
SF16 2	1.07537	148.893	22169.13213	0.6742335
SF16 3	1.08100	148.5151	22056.83250	0.68046699
SF16 4	1.06607	149.5205	22356.38830	0.65156541
SF16 5	1.03132	151.8978	23072.92514	0.61518989
SF16 6	0.99411	154.502	23870.87655	0.5374226
SF16 7	0.92853	159.2464	25359.41112	0.7846189
SF16 8	0,82997	166.7668	27811.1616	1.1936277
SF32 1	1.09412	147.6397	21797.48757	0.6760410
SF32 2	1.07537	148.893	22169.13214	0.6742335
SF32 3	1.08100	148.5154	22056.83250	0.68046699
SF32 4	1.06607	149.5205	22356.38830	0.65156541
SF32 5	1.03132	151.8978	23072.92514	0.61518989
SF32 6	0.99411	154.502	23870.87655	0.5374226
SF32 7	0.92853	159.2464	25359.41112	0.7846189
SF32 8	0.82997	166.7668	27811.16169	1.1936277

7- Conclusion

This paper presents a propos of new cryptography algorithm which prevents attacker from detecting images across internet networks .

It can use decomposed image in bit plane method and uses compression method with secure force algorithm, these three steps to make the new algorithm more secure, and it does not where any attacker to observe and analyze information on images existence.

The results obtained from this algorithm cryptography its efficiency, power, and high security. From comparing original image of image decomposed with image of wavelet and secure force. Distortion measure is obtained in PSNR, RMAE, MSE, and correlation between them.

The PSNR in original image is 0.9486 , the range of bit plane is from 1.0218 to 1.8126, the range of wavelet16 is from 0.70133 to 1.8765, the range of wavelet32 0.71338, the range of SF16 is from 1.09412 to 0.7820, and the range of SF32 1.03721,……RMES, …..MSE, ……etc. in Tables (1), Table (2), and the range of correlation in original image is from 3.466496 to SF32 7.9157052.

References:

1- Shujaat Khan, M. Sohail Ibrahim, Kafeel Ahmed Khan, and Mansoor Ebrahim , " Security Analysis of Secure Force Algorithm for Wireless Sensor Networks ", Asian Journal of Engineering Science and Technology 2015.

2- John C. Russ, "the Image Processing Handbook", A CRC Handbook Published in Cooperation With IEEE Press, Third Edition, 1998.

3- Tinku Acharya, and Ajoy K. Ray, " Image Processing Principles and Applications", Published by John Wiley & Sons, Inc., Hoboken, New Jersey, 2005.

4- Rafael C. Conzalez, and Richard E. Woods, "Digital Image Processing" , Prentice Hall, Second Edition, 2001.

5- N. S. T. Sai, and R. C. Patil, "Image Retrieval Using Bit-Planr Pixel Distribution", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011.

6- Anuj Bhardwaj, and Rashid Ali, "Image Compression Using Modified Fast Haar Wavelet Tansform", World Applied Sciences Journal 7 (5): 647-653, 2009.

7- V.Ashok, T.Balakumaran, and C.Gowrishankar," The Fast Haar Wavelet Transform for Signal & Image Processing", (IJCSIS) International Journal of Computer

Science and Information Security, Vol. 7, No. 1, 2010.
8- Elminaam, D. S. A., Abdual-Kader, H. M., and Hadhoud, M. M., "Evaluating The Performance of Symmetric Encryption Algorithms IJ Network Security", 10(3), 216-222, 2010.
9-