ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Simple Logic Operation Based Mixed Protection Archived Medical Images Method

Bashar Jabbar Hamza [1]

Senior Lecturer, Department of Communications Techniques Engineering, Engineering Technical College- Najaf,

Al-Furat Al-Awsat Technical University, Najaf, Iraq[1]

ABSTRACT: Safeguard of different information types from attackers is paramount for human societies. Keeping image secret is a big problem because it has large amount of data. Also, the pattern appearance problem in medical image especially in background image is another important difficult that facing image security algorithms. A combining ciphering with hiding techniques based mixed security algorithm is introduced in this paper. BCD decomposition, reordering, and scrambling are three operations executed on the secret image before hide it in cover image using simple LSB operation in introduced hiding technique. The stego-image result from proposed hiding technique is ciphered using improved encryption algorithm to get mixed security algorithm. The visual scene, histogram analysis, entropy, security analysis, and execution time are factors used to evaluate the performance of suggested algorithm.

KEYWORDS: Medical image encryption, Multimedia steganography, Multimedia processing, Mixed security.

I. INTRODUCTION

Safeguard of different types of information from attackers is paramount for people and governments. High levels of security is important in security methods to protect the patients privacy through protect them data base such as archived images. In digital multimedia, ciphering and hiding are both aimed to safeguard the data from adversaries. Encryption techniques effectively protect multimedia information through converting it into scrambled form which undefined by attackers [1-3]. Generally, frequency and spatial domains are to forms used to represent a digital image, where it can be encrypted partially or fully in two obviously domains [4]. Fractional Fourier Transform "FrFT" [5; 6], Fast Fourier Transform "FFT"[7], Discrete Cosine Transform "DCT" [8], or Fresnel Transform "FrT" [9; 10] are image encryption approaches in the frequency domain. Most of the ciphering algorithms in the frequency domain are dependent on the coefficients of those transforms, where the secret image is protected through ciphering its coefficients which get it through applying one of those transformers.

Image encryption in the spatial domain based on changing the pixel value"diffusion", and/or the pixel location"confusion" to get image in incomprehensible form [11]. Based on simplicity and computational cost the encryption image represented in the spatial domain is more effective than ciphering image represented in the frequency domain [12,13]. Several ciphering approaches are introduced based on chaos theory [14; 13; 8; 15; 16;17]. However, chaos theory- based ciphering algorithms are not very secure and require additional computations [18]. Images decomposition technique is used recently in many ciphering algorithms [19; 20; 21; 22]. Unfortunately, One of important drawbacks in decomposition based image ciphering is the atonality in the security level because the number of bit planes and the content of each bit plane are constant. Additionally, key space is little or in some cases not exist, so, computational costs of the attacks are decreased.

In this paper, a mixed image security algorithm is introduced based on a combination of encryption and hiding mechanisms. A new hiding algorithm is proposed based on simple logic operation and LSB to hide the secret image in an unknown scene cover image. The improved version of BCDEA algorithm proposed in (37) is used to encrypt the stego-image that is produced from the proposed hiding algorithm.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The remainder of this paper is organized as follows: Section II shows the related works. Section III reviews proposed approach ., the experimental results and conclusions are drawn in Secs IV & V .

II. RELATED WORK

Before about six to seven decades , the idea of absence the appearance of information sent, which called "information hiding" was widely used [23]. So, information hiding can be defined as concealment important information into a cover such as an image, video or audio [24]. Generally, there are two groups of dissimulation approaches are steganography and digital watermarking. Steganography is the mechanism that hide secret information in a host media such that the secret massage in the stego-media becomes invisible to the eavesdropper [25]. Whilst, the hidden secret information in digital watermarking is visible but an attacker cannot supplant or change the hidden information from the watermarked media [26].

Famous and older technique for images steganography in the spatial domain is LeastSignificantBit(LSB), which is replacing the LSBPlane of the host image with secret image bitplanes. A number of methods have been proposed to improve the performance of the LSB technique, such as LSB matching (LSBM) [27] and LSB matching revisited [28] (LSBMR) . Additionally, the hiding capacity of LSB, LSBM, and LSBMR is small, partially because these methods address a given pixel or pixel pair without considering the relationship between neighboring pixels. Several methods that were proposed are based on differencing between neighboring pixels to separate between edge and smooth regions and hide secret bits at different rates in those regions adaptively [29; 30]. On the other hand, some methods have suggested enhancing the quality of the stego-image that results from the LSB replacement technique by applying an optimal pixel adjustment process (OPAP), which depends on the difference between the cover and stego pixel values [24; 31].

However, the hiding and ciphering techniques cannot achieve the optimal case of data protection using any one of them alone. As a result, a hybrid system between them was suggested by many researchers to produced multi-layer security. Dinku A Adale proposed in [32] two hybrid systems that were called as Crypto-Steg and Steg-Crypto using short key length RSA encryption and LSB insertion embedding methods. B. Karthikeyan et al suggest a simple hybrid security method based on applying the XOR operation between the plaintext and randomly generated key before hiding it in a cover image using the LSB technique [33]. Nameer N. EL-Emam proposed a hybrid security algorithm using three layers of security [34]. These three layers were encrypting the plain text using AES or DES, segmenting the cover image adaptively, and selecting pixels that carry the secret data. Another hybrid security methods were proposed in [22, 35, 36] using different encryption algorithms and hiding techniques. However, all of the previous hybrid methods used the LSB technique for hiding purposes, which impairs their performance.

III. PROPOSED METHOD

Mixed Hiding and Ciphering Image Protection Method (MHCIP):

The security levels of most hybrid algorithms suffer from weakness as results to use the LSB as hiding part which makes these methods susceptible to attacks by a number of adversaries [22]. So, this work introducing a new mixed security algorithm based on a new high capacity hiding techniques and enhanced encryption algorithm. Two parts of suggested MHCIP method are shown in sub sections below:

1- A New Hiding Technique (Hiding based Logic Operation HbLO):

The HbLO is a lossy steganography method because it loses the two least significant bit planes of the secret image. The binary bit planes secret image will be reordered and scrambled before hide it in unknown scene cover image to increase the hiding capacity.

In general, 8-bit grey-scale images are represented by 8 bit planes when decomposed using binary system, whilst, need 12 bit planes if the BCD code used to decompose the 8-bit gray scale secret image. Important to know how many binary bit planes that can be lost with keeping reconstructed image with high quality. Obviously, at least 5 MSBs are required to reconstruct the decomposed image with approved levels of quality [37**]**. Therefore, 6 MSBPs will be used from the secret image to reconstruct it with high quality.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The **HbLO** is explained in steps below:

1. Decomposing the secret image to binary bit planes based on Eq. (1)

$$D = \sum_{i=0}^{n-1} a_i 2^i = a_0 2^0 + a_1 2^1 + a_2 2^2 + a_3 2^3 \quad (1)$$

where codes (a_3, a_2, a_1, a_0) are the binary representation of the non-negative digit D in decimal number.

A 8-bit gray scale image pixel is represents in range (0-255) so the BCD code representation of each pixel is 12 bit. The 4-bits of first digit of pixel value can be neglected which mean change the pixel value in range (0-9), where this range don't more effect on the image quality. On the other hand, the Most Significant Digit value in range (0-2), so, this digit represented into two bits only and other two bit is neglected. Finally, each pixel represented in 6 bits only.

2. Reordering the 6 bitplanes (5^{th}, 6^{th}, 7^{th}, 8^{th}, 9^{th}, & 10^{th} bitplanes) of the secret image using Eq. (2):

$$P_{sa}(c) = P_{sb}(a + b \bmod 12) \quad (2)$$

where P_{sb} and P_{sa} are the bit planes of the secret images before and after reordering, respectively; and (a=10, 9… 5), b is a number defined between transmitter and authenticated receiver.

3. Scramble the reordered bit planes through applying the gray code on bitplans separately.
4. hide the scrambled bitplanes in unknown cover image using LSB technique to get stego-image.

2- Binary Codes based Image Encryption Method(BCIE):

A simple speedy image encryption algorithm based on binary codes is introduced in this paper as second part of MHCIP method. The proposed encryption method has several steps in two stages, where first stage applied on image after decompose it to binary bit planes. These steps are reordering, scrambling, then reconstructing image to pixel values. Whilst, steps of second stage are (AddRounKey, ShiftRow, SubByte, AddRoundKey) applied on image pixels after reconstruct it from first stage. Points below show the suggested encryption method steps for two stages:

Stage 1

1. Decompose the stego-image resulted from hiding operation to binary bitplanes based on Binary codes (the weights of binary codes known by authenticated persons only). The pixel value range in 8-bit gray scale image is (0-255), so each digit will decomposed alone in one pixel. The weight suggested in this paper is (11 4221 6321)
2. Reorder bitplanes resulted from step1 based on Eq. 2 but change the value of (a=12, 11… , 2, 1).
3. Scramble the reordered bit planes through applying the gray code on bitplans separately.
4. Reconstruct image from scrambled bitplanes that results from step3 by using same binary codes weights shown in step1.

Stage 2

1. Divide the image results from stage1 to blocks in 4×4 pixels for each block.
2. Apply first AddRoundKey operation which executed through carryout EX-OR operation between image block and secret key (Secret key is 128 bit key divided into 16 byte arranged in 4×4 matrix).
3. Shift the pixels of matrix results from step2 using same ShiftRow operation applied in Advanced Encryption Standard (AES) algorithm.
4. Apply the substitution step which means substitute each pixel of matrix results from step3 in a 16×16 matrix called S-Box that suggested in (37).
5. Apply 2nd AddRoundKey operation between matrix results from step4 and 4×4 block from image called KeyImage which it is secret between authenticated persons only.
6. Repeat the steps2-5 ten times for each block of image results from stage 1.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

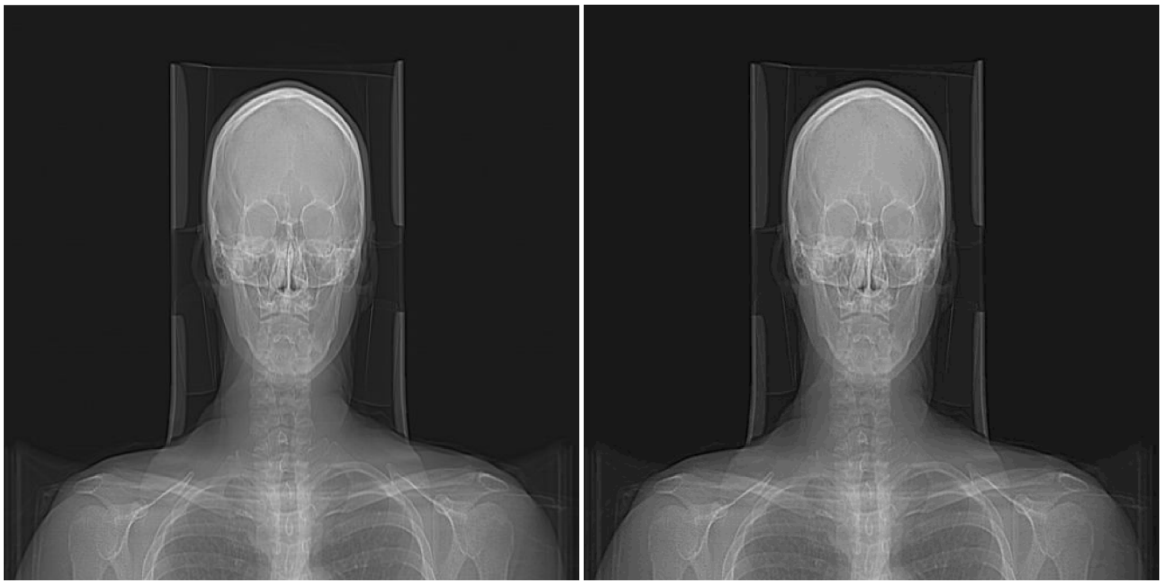
Vol. 6, Issue 2, February 2017

IV. EXPERIMENTAL RESULTS

Four medical image in 512×512 dimensions are used as tests image to evaluate the performance of proposed mixed Mixed Hiding and Ciphering Image Protection Method (MHCIP). Several parameters are used to test the performance of MHCIP such as similarity between original and reconstructed versions of secret image, security analysis, and execution time. The performance test depends on evaluation only without any validation and comparison with another hybrid algorithms because all reviewed algorithms so far in mechanism from introduced algorithm in this paper. Medical images have a challenge against image protection algorithms where, the background regions of medical image it is so much regions with same colour which make much problem for image security algorithm. The subsections below review the performance test of suggested MHCIP algorithm.

1- Similarity Test:
This factor is important to tested because part of mixed algorithm proposed is hiding operation which is lossy hiding technique, so need to check the similarity between original image and final reconstructed image from stego-image. The similarity will checked through visual scene, peak signal to noise ration, SSIM, Q-index and PPCC as below:

A- The visual scene: here, naked eye will be used to check whether the original and extracted secret images are identical for the 4 test images. Fig. 1 shows that the human eyes cannot be sensitive any differences between the original and extracted images for the all sample images tested. That means, the losed information in hiding technique don't effect on the visual scene of secret image.



(a)

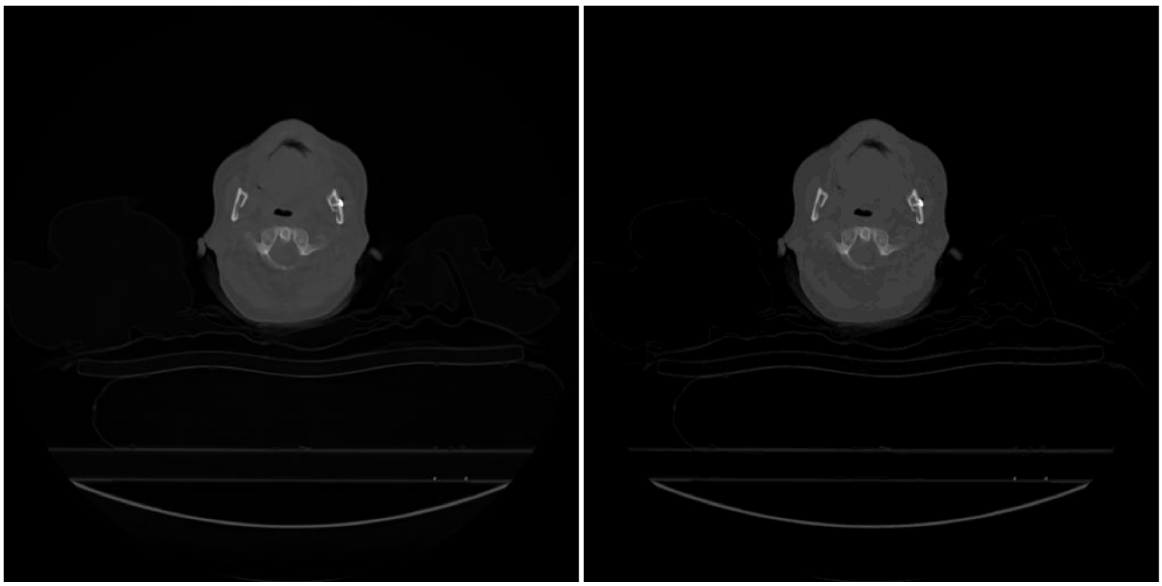
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

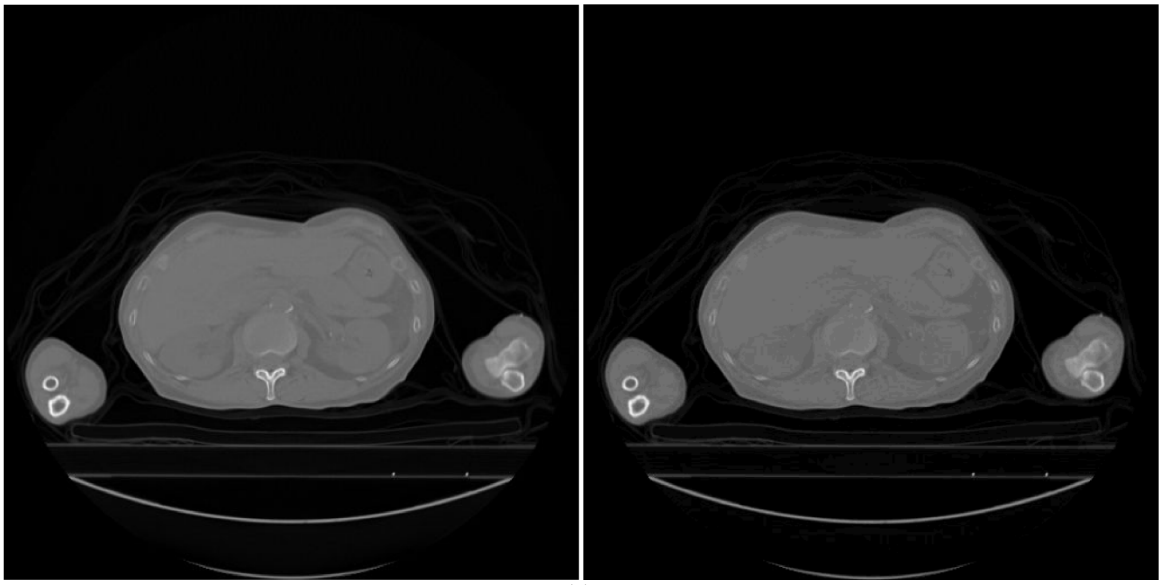
(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017



(b)



(c)

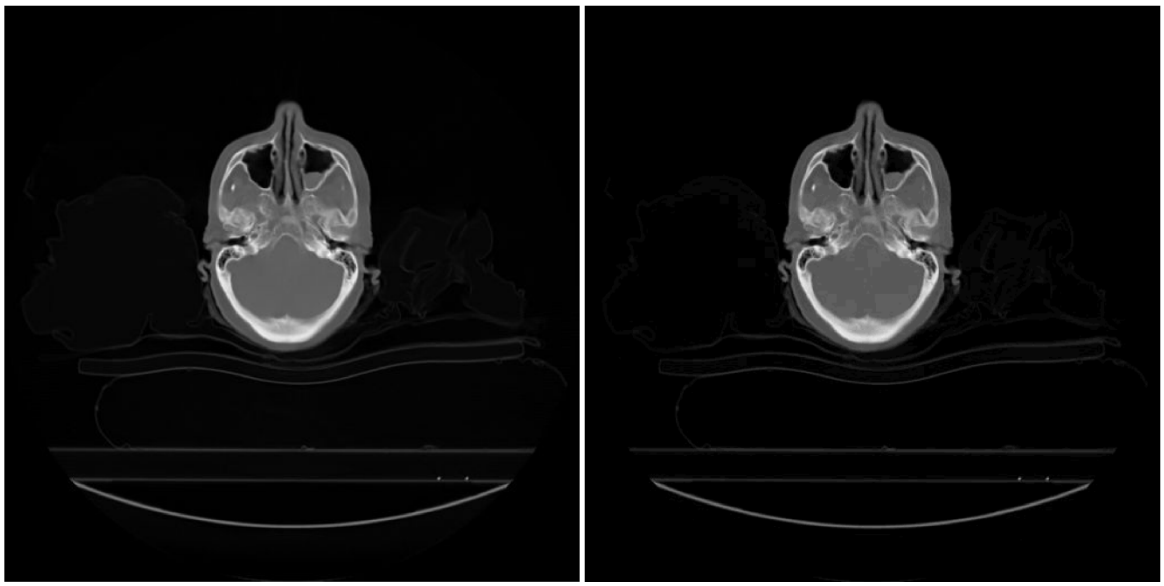
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017



(d)

Fig. 1. The Original and Reconstructed of Secret Image Medical (512×512): 1st & 2nd columns are original & reconstructed image; a) Test1; b) Test2; c) Test3; d) Test4.

B. Peak Signal to Noise Ratio PSNR: The PSNR is one of the parameters that are used to check the image similarity. If the two tested images are identical, then the PSNR is equal to infinity; also, if the value of the PSNR is more than 30 dB, then the human eyes cannot be sensitive any difference between the tested images [31]. Table 1 shows the values of PSNR for the four tests, where its value conforms that the similarity of the original and extracted image in the allowable ranges.

C. SSIM, Q-index, and PPCC: These are other parameters used to measure the similarity between two images. The range value of these parameters is in the range of 1 to -1, where identical images have the value 1 for all of the parameters. The values of SSIM, Q-index, and PPCC for all of the tested images are shown in Table 1. The results of those three parameters confirm the similarity between the original and extracted images, where, those values are very near 1.

Table1 Statistical Measurements of Images Similarity Between Original and Extracted Images For (MHCIP).

The tests images	Parameters			
	PSNR	SSIM	Q-index	PPCC
Test1(Medical 512×512)	39.4351	0.9525	0.9772	0.9641
Test2 (Medical 512×512)	37.5723	0.9686	0.9751	0.9872
Test3 (Medical 512×512)	38.8791	0.9592	0.9824	0.9771
Test4 (Medical 512×512)	39.5718	0.9451	0.9761	0.9762

2- Security Analysis:

The security of the mixed algorithm will be analyzed and evaluated using several parameters visual scene, histogram analysis, correlation coefficients, key space, effect of noise attacks and entropy.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

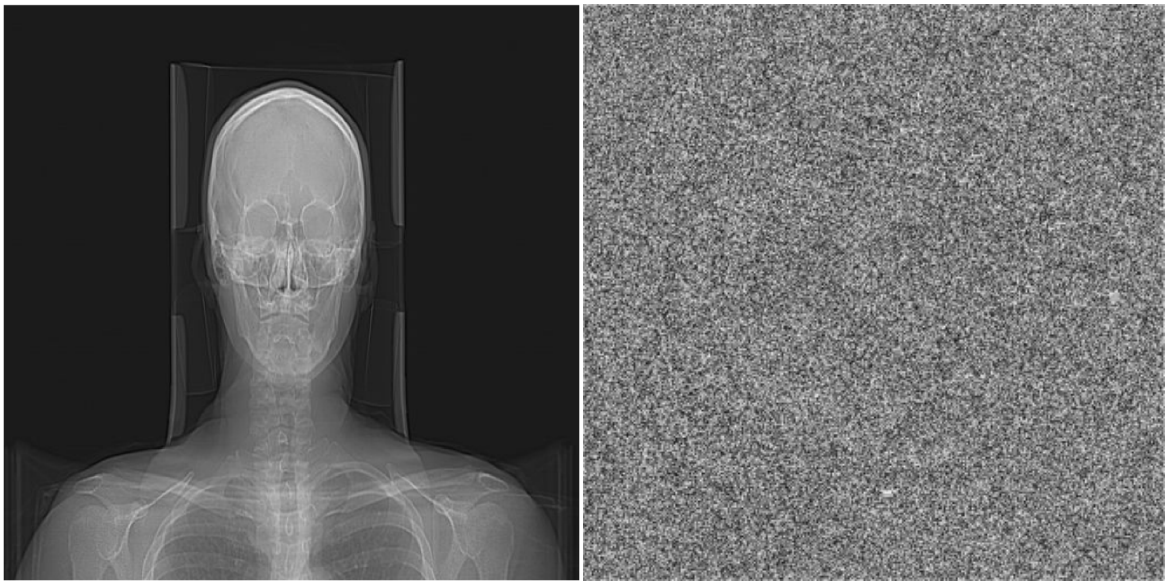
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

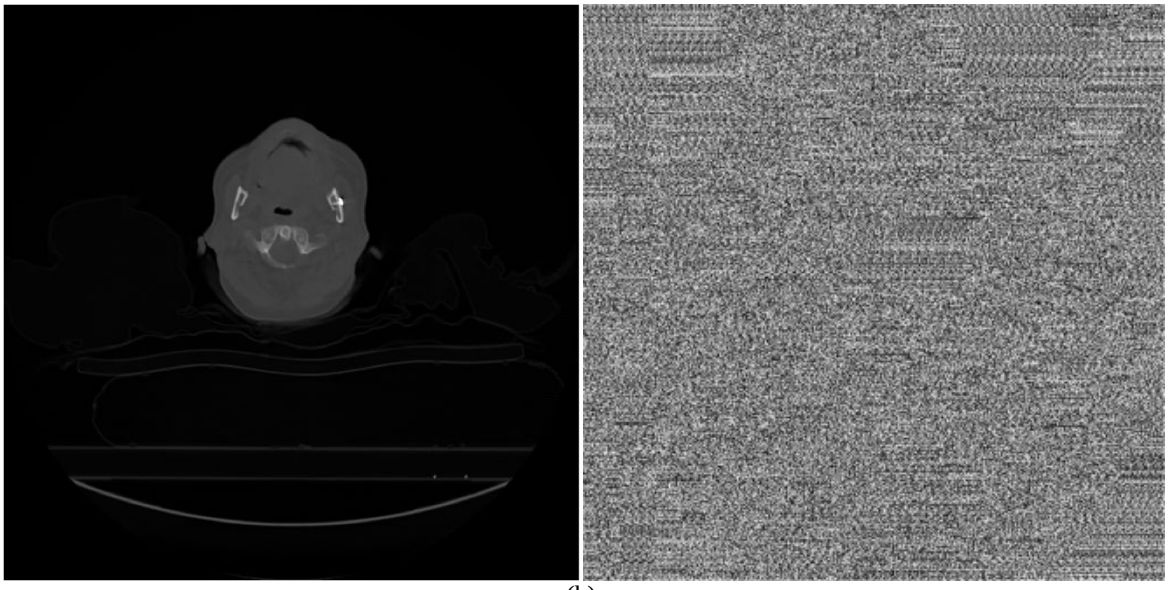
Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

A. Visual scene: The visual scene of protected image will be shown for four tests image. The scene of image resulted from MHCIP method proposed is should be like jamming scene in TV which it is preferred scene for ciphered image because part of the proposed approach is ciphering technique in additive to that the cover image is unknown scene image. Figure 2 shows the visual scene of original and protected images by suggested method for four tests. As clearly appear in figure, the introduced method achieved the first security condition for visual scene of protected image.



(a)



(b)

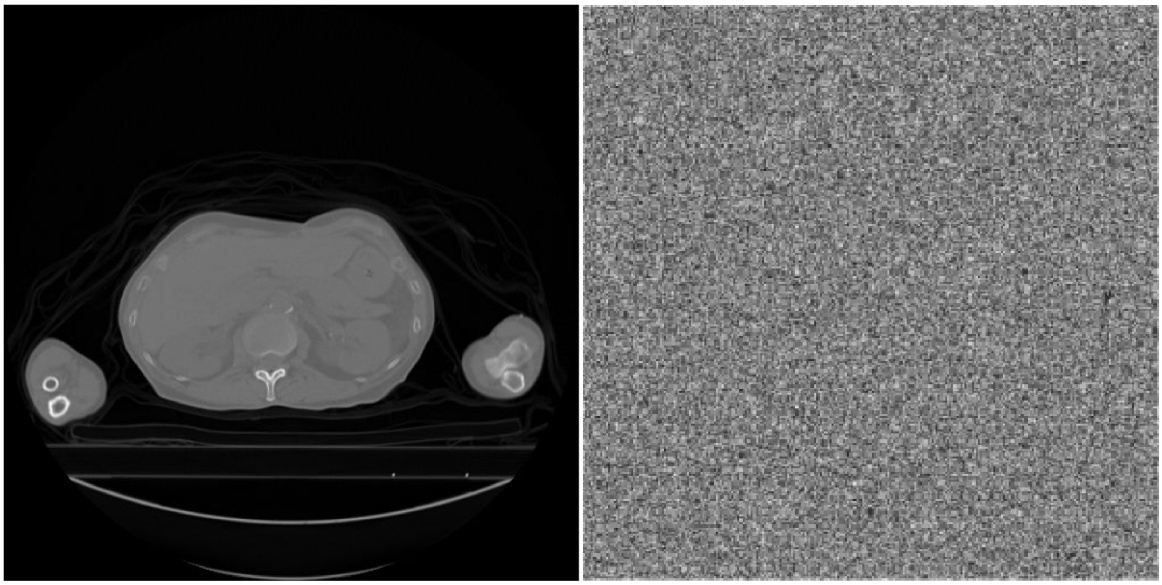
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

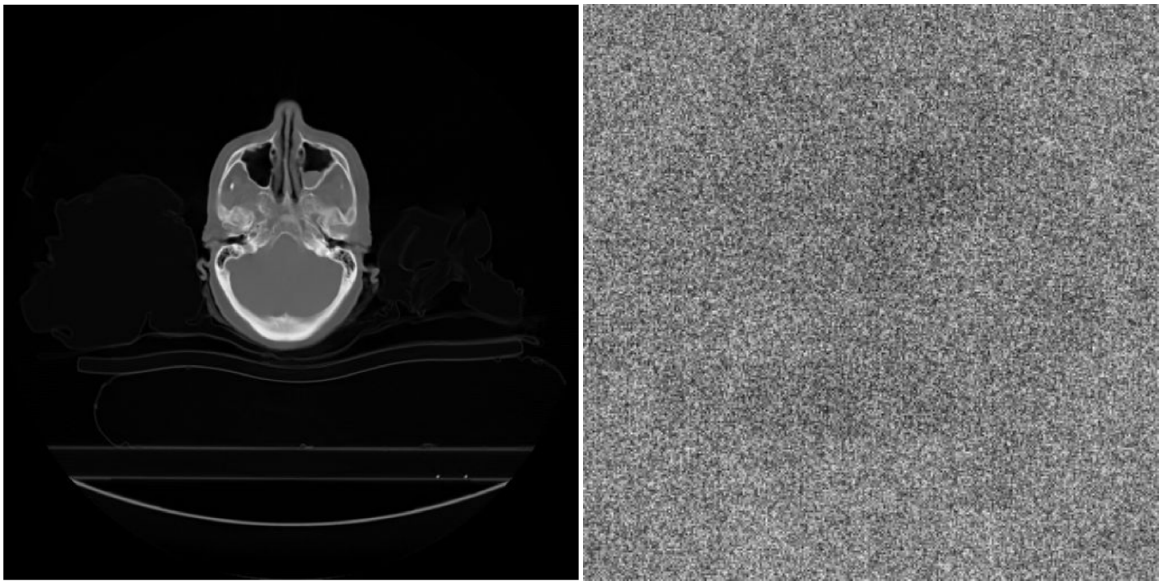
(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017



(c)



(d)

Fig. 2. The Original and Protected Image by MHCIP Medical (512×512): 1st & 2nd columns are original &protected images respectively; a) Test1; b) Test2; c) Test3; d) Test4.

B. Histogram Analysis: The second parameter used to evaluate the performance of the mixed MHCIP algorithm is the histogram analysis which gives good indicators for statistical attacks. The results appearing in Fig. 3 clearly show that the histogram of the mixed algorithm was uniformly distributed for all tests.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

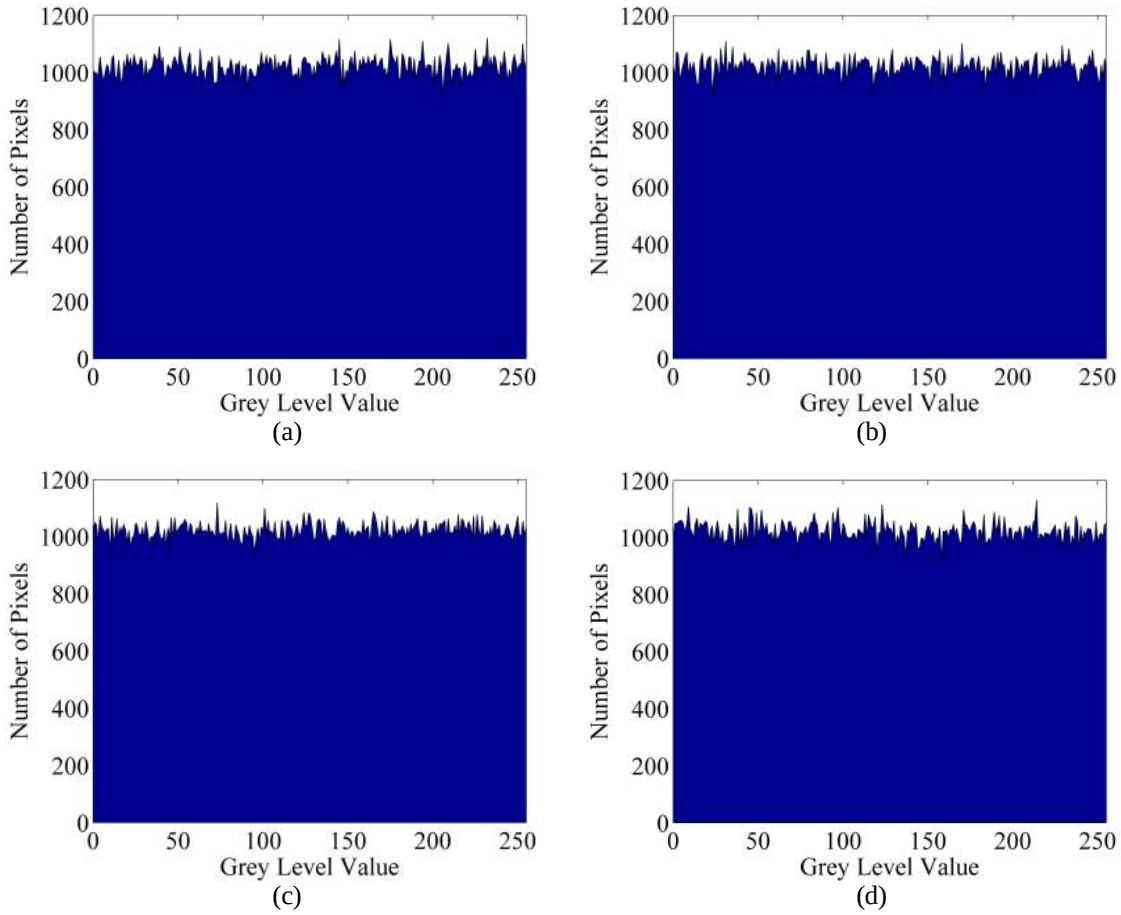


Fig.3. Histogram Analysis of Protected Images by Mixed MHCIP Algorithm for Four Tests Medical (512×512): (a) Tes1; (b) Test2; (c) Test3; (d) Test4.

C. Correlation coefficients: The correlation coefficients of the protected image by the proposed mixed MHCIP method for four test images are shown in Figure 4. As shown in Figure 4 (a)-(d), the proposed method produces a protected image with very low correlation between adjacent pixels. The statistical values of correlation coefficients of the protected image by the suggested method are shown in Table 2. The values of correlation coefficients in Table2 is much low for all tests which means that the MHCIP method is safe against statistical attacks.

Table 2. Correlation Coefficients of Original and Protected Images by Mixed MHCIP for 4 Tests.

Type of image	Test1 Medical(512×512)	Test2 Medical(512×512)	Test3 Medical(512×512)	Test4 Medical(512×512)
Original image	0.951	0.972	0.990	0.969
MHCIP algorithm	0.002	0.006	0.014	0.005

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

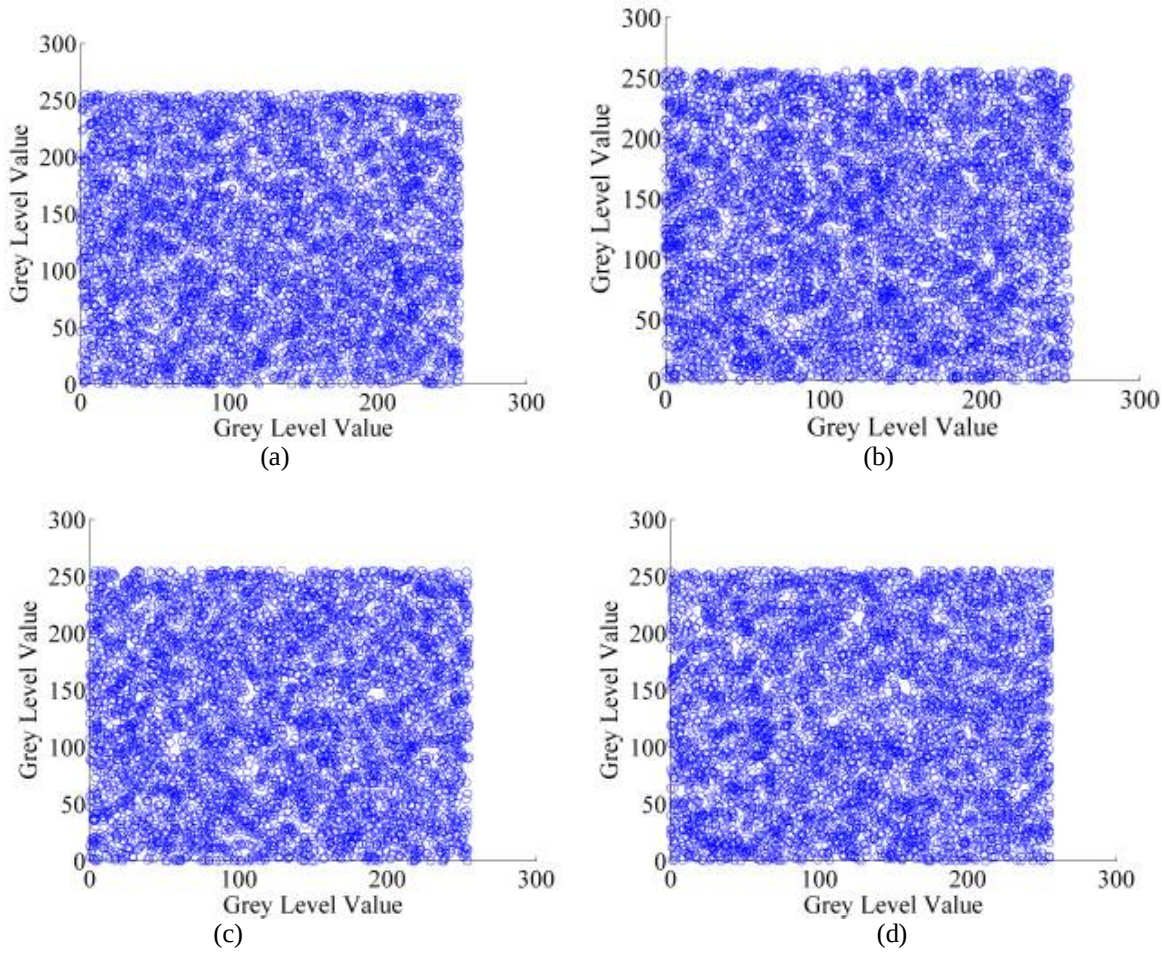


Figure 4: Correlation Coefficients of Protected Image by Mixed MHCIP for Four testsMmedical (512×512): (a) Test1; (b) Test2; (c) Test3; (d) Test4.

D. **Entropy**: the entropy values of the original and MHCIP method are shown in Table 3 for the four tests images. The results in Table 3 show the entropy values for the mixed MHCIP method are nearest to 8. The results of the histogram analysis, correlation coefficients and entropy prove that the proposed mixed approach is strong against statistical attacks.

Table 3: Entropy values of original and protected images by mixed MHCIP method for 4 tests.

Type of image	Test1 Medical(512×512)	Test2 Medical(512×512)	Test3 Medical(512×512)	Test4 Medical(512×512)
Original image	5.038	5.353	3.919	4.235
MHCIP method	7.998	7.997	7.995	7.999

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

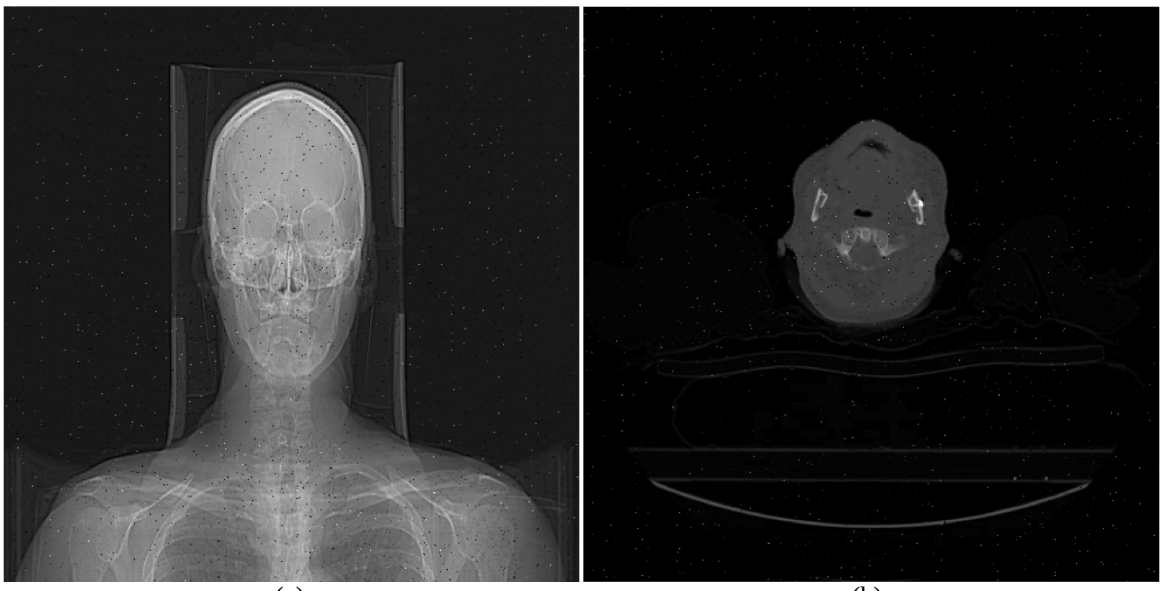
(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

E. Noise attacks: the performance of suggested algorithm also tested against noise attackers. Sault noise in percentage about 5% are add to protected image then re-extracted it to study the effect of noise attacks on the protected image by mixed MHCIP method. Same tests images were used in this evaluation. SSIM was used to measure the similarity between the original and reconstructed images. Figure 5 shows the reconstructed image from protected noised images for all tests. The visual scene and values of statistical parameters prove that the mixed MHCIP method is strong against this type of attacks.

F. Data loss problems: the performance of proposed algorithm tested against data loss problems too. A data in first corner, center and last corner of protected image are reset with dimensions (10×10) pixels in each corner. Same tests images were used in this test. Also, SSIM, Q-index, PPCC and PSNR was used to measure the similarity between the original and reconstructed images. Figure 6 shows the reconstructed image from protected data losed images for all tests. The visual scene and values of statistical measuring proved the mixed MHCIP method is strong against this type problems.



(a) (b)

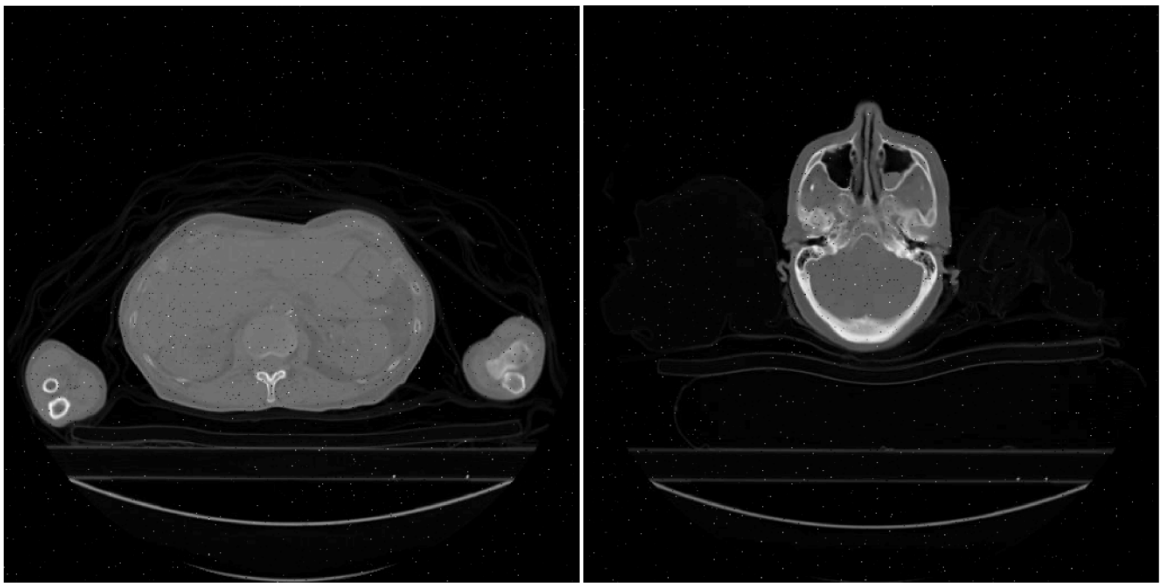
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

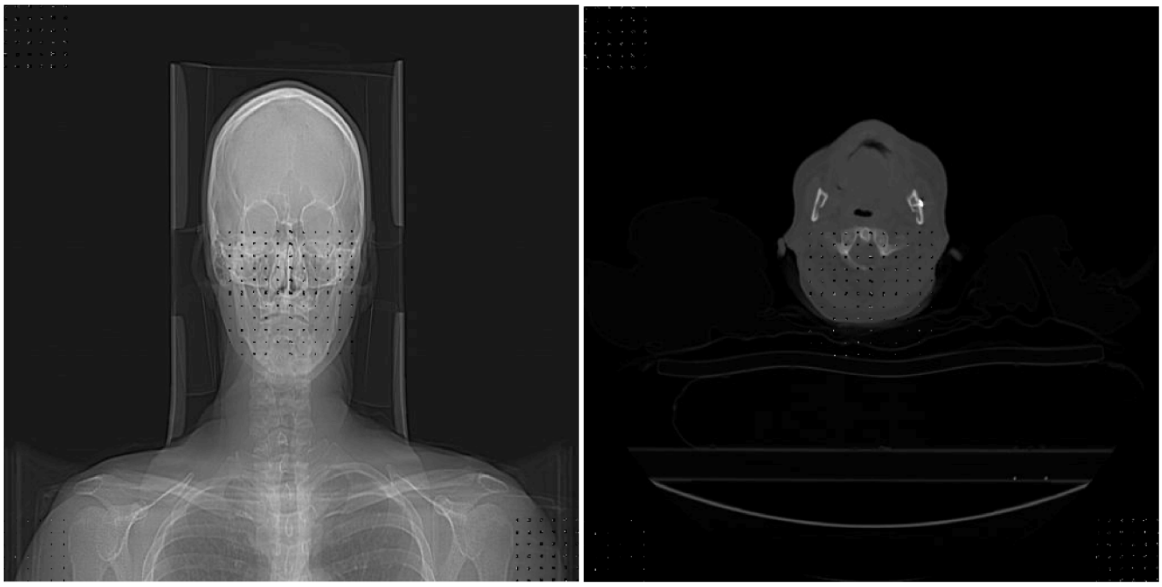
Website: www.ijirset.com

Vol. 6, Issue 2, February 2017



(c) (d)

Figure 5: Noise Attacks test of Protected Image by Mixed MHCIP for Four Tests Medical (512×512): (a) Test1; (b) Test2; (c) Test3; (d) Test4.



(a) (b)

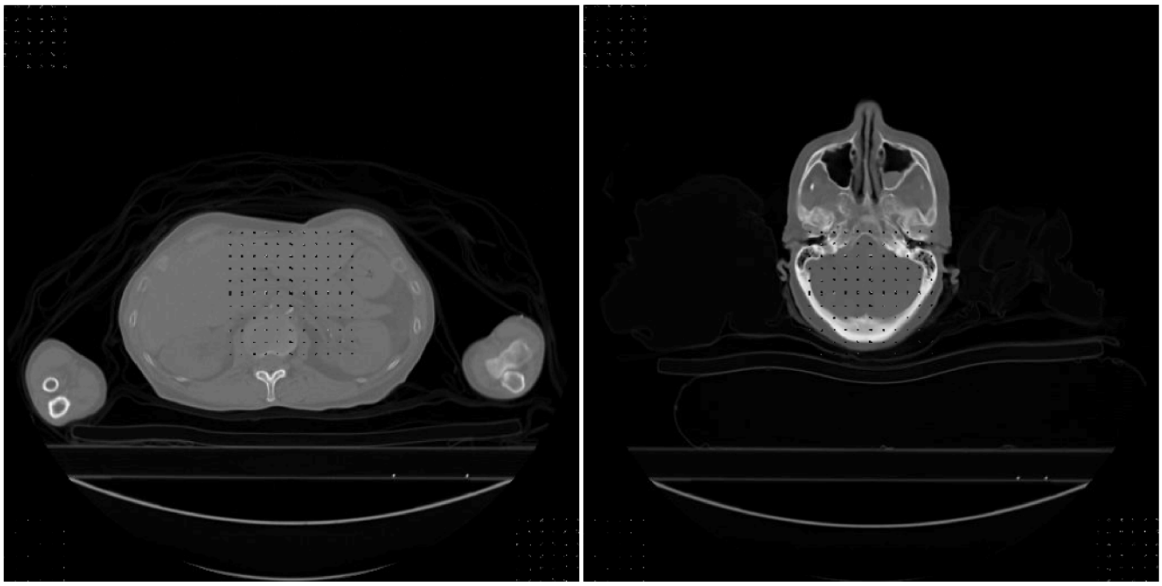
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017



(c) (d)

Figure 6: Data Loss Attacks Test of Protected Image by Mixed MHCIP for Four Tests Medical (512×512): (a) Test1; (b) Test2; (c) Test3; (d) Test4.

Table 4 shows the value of statistical measurements of Noised and data losed images for four tests images.

Table 4: Statistical parameters values of noised and data losed image for four tests images.

Image	Noised Extracted Image				Data losed Extracted Image			
	PPCC	SSIM	Qindex	PSNR	PPCC	SSIM	Qindex	PSNR
Test1 (Medical 512×512)	0.9934	0.9953	0.9964	28.7562	0.9978	0.9956	0.9985	29.8452
Test2 (Medical 512×512)	0.9981	0.9931	0.9961	28.8165	0.9954	0.9925	0.9947	30.0012
Test3 (Medical 512×512)	0.9851	0.9901	0.9892	28.0371	0.9906	0.9891	0.9801	29.8964
Test4 (Medical 512×512)	0.9942	0.9951	0.9945	39.1103	0.9927	0.9975	0.9965	29.7251

G. Key Space: the key space of proposed mixed MHCIP method combine between HbLO & BCIE key space. The hiding algorithm key space results from (b number which it is any correct positive number) in reordering operation as in Eq. 2. Whilst, the key space of BCIE results from 128 bit key in first AddRoundKey stage and (M×N)×8 bits results from 2nd stage of AddRoundKey. Equation 3 below shows the key space of suggested mixed MHCIP method.

$$KS = 2^{128} \times 2^{M \times N} + b = 2^{128+(M \times N)} + b \quad (3)$$

where *M* and *N* are key image dimensions, b is the correct positive number. From Equation (3), the key space is very large and cannot take all possibilities cases for all key space. Therefore, the mixed MHCIP approach is very strong against brute force attack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

V. CONCLUSION

This paper aimed to introduce high efficiency image security algorithm for image in medical applications. The suggested method is mixed image security algorithm between hiding and ciphering techniques. The first part of mixed MHCIP method that introduced in this paper is a new high capacity hiding algorithm called HbLO, which is based on simple logic operation to hide an image in another image that has the same dimensions. An unknown scene image is used as a cover image in the HbLO method to increase the hiding capacity. Whilst, the second part of mixed MHCIP algorithm is the BCIE ciphering algorithm which it is an improved of BCDEA ciphering algorithm.
The mixed MHCIP method is carryout in two stage, 1st stage is hiding 6 MSBPs of the secret image after reordering and scrambling them in unknown scene cover image using simple LSB technique. On the other hand, the 2nd stage is encrypting the stego-image results from 1st stage using BCIE encryption algorithm. The BCIE method is very speedy consist of 4 steps repeated ten times to increase the security levels spatially against burst attacks. The Steps of BCIE are 2 AddRundKey operations, ShiftRow, and SubByte. The performance of mixed MHCIP algorithm is evaluated based on two important factors are similarity between original and reconstructed images and security analysis. First factor is important because the hiding method is lossy hiding technique, so need to check the quality of reconstructed image. The second factor (security analysis) is tested through several parameters such as visual scene of protected image, statistical measuring (Correlation coefficients, PPCC, Q-index, SSIM, and entropy), noise attacks, data loss attacks, and key space. The results of all parameters proved that the mixed MHCIP method is very well archived protecting image through security levels and execution speed.

REFERENCES

[1] Akhshani, A., Behnia, S., Akhavan, A., Hassan, H. A., Hassan, Z., "A novel scheme for image encryption based on 2d piecewise chaotic maps", Optics Communications, Vol. 283, no. 17, pp. 3259-3266, 2010.
[2] Sudharsanan, S., "Shared key encryption of jpeg color images", IEEE Transactions on Consumer Electronics, Vol.51, no.4, pp.1204-1211, 2005.
[3] Podesser, M., Schmidt, H., Uhl, A., "Selective bit-plane encryption for secure transmission of image data in mobile environments", 5th Nordic Signal Processing Symposium on board Hurtigruten, Anjuran Norway, 2002.
[4] Moon, D., Chung, Y., Pan, S., Moon, K., Chung, K., "An efficient selective encryption of fingerprint images for embedded processors", ETRI Journal , Vol.28, no.4, pp.109-118, 2006.
[5] Fan, G., Chen, L., Zhao, D., "A half-blind color image hiding and encryption method in fractional Fourier domains", Optics Communications, Vol.281, no.17, pp.4254-4260, 2008.
[6] Zhou, N., Wang, Y., Gong L., "Novel optical image encryption scheme based on fractional mellin transform", Optics Communications, Vol.284, no.13, pp.3234-3242, 2011.
[7] Borujeni., S. E., "Speech encryption based on fast Fourier transform permutation", The 7th IEEE international conference on electronics, circuits and systems. Jounieh-Lebanon, pp.290-293, 2000.
[8] Liu, H., Wang X., "Color image encryption using spatial bit-level permutation and high-dimension chaotic system", Optics Communications, Vol.284, no.16–17, pp.3895-3903, 2011.
[9] Chang, T., Hwang, E., Lee, C., "Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain", Optics Communications, Vol.284, no.18, pp.4146-4151, 2011.
[10] Hone, H., "An optical image cryptosystem based on Hartley transform in the Fresnel transform domain", Optics Communications, Vol.284, no.13, pp.3243-3247, 2011.
[11] Chong, F., Miao, Y., Liu, X., Chen, J., "A novel chaos-based bit-level permutation scheme for digital image encryption", Optics Communications, Vol.284, no.23, pp.5415-5423, 2011.
[12] 12. Schneier, B. (1996). Applied Cryptography. John Wiley & Sons.
[13] Li, X., Cho, S., Kim, S., "Computational integral imaging-based 3d digital watermarking scheme using cellular automata transform and maximum length cellular automata", Multidimensional Systems and Signal Processing, Vol.25, no.3, pp.405-424, 2014.
[14] Akhavan, A., Samsudin, A., Akhshani, A., "A symmetric image encryption scheme based on combination of nonlinear chaotic maps", Journal of the Franklin Institute, Vol.348, no8, pp.1797-1813, 2011.
[15] Borujeni, S., Eshghi, M., "Chaotic image encryption system using phase-magnitude transformation and pixel substitution", Telecommunication Systems, Vol.52, no.2, pp.525-537, 2013.
[16] Ye, R., "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism", Optics Communications, Vol.284, no.22, pp.5290-5298, 2011.
[17] Zhu, Z., Zhang, W., Wong, K., Yu, H., "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences, Vol.181, no.6, pp.1171-1186, 2011.
[18] Alexander, N., Pisarchik, M., "Chaotic map cryptography and security", In Nova Science Publishers. Encryption: Methods, Software and Security, pp.301-332, 2012.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

[19] Chen, L., Zhao, D., Ge, F., "Image encryption based on singular value decomposition and Arnold transform in fractional domain", Optics Communications, Vol.291, no.0, pp.98-103, 2013.
[20] Jiancheng, Z., Ward, R., Dongxu Q., "A new digital image scrambling method based on Fibonacci numbers", Proceedings of the International Symposium on Circuits and Systems (ISCAS 04), Vol.3, pp.965-968, 2004.
[21] Zhou, ., Panetta, K., Agaian, S., "Image encryption algorithms based on generalized p-gray code bit plane decomposition", The Forty-Third Asilomar Conference on Signals, Systems and Computers, pp.400-404, 2009.
[22] Wei, Z., Cheng, Z., Cui, Y., "Image data encryption and hiding based on wavelet packet transform and bit planes decomposition", The 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp.1-4, 2008.
[23] Moulin, P. & Koetter, R., "Data-hiding codes" Proceedings of the IEEE, Vol.93, no.12, pp.2083-2126, 2005.
[24] Chan, C. K., & Cheng, L. M., "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.37, no.3, pp.469-474, 2004.
[25] Wu, D. & Tsai, W., "A steganography method for images by pixel-value differencing", Pattern Recognition Letters, Vol.24, no.9–10, pp.1613-1626, 2003.
[26] Cox Ingemar J., Leighton F., Shamoon T., "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, Vol.6, no.12, pp.1673-1687, 1997.
[27] Han, J., Park, C., Ryu, D., Kim, E., "Optical image encryption based on X-OR operations", Optical Engineering, Vol.38, no.1, pp.47-54, 1999.
[28] Mielikainen, J., "LSB matching Revisited", IEEE Signal Processing Letters, Vol.13, no.5, pp.285-287, 2005.
[29] Hempstalk, K., "Hiding behind corners: using edges in images for better steganography", Proceedings of the Second Computing Women Congress (Cwc 2006): Student Papers, Hamilton, New Zealand, pp.5-7, 2006.
[30] Weiqi, L., Fangjun, H., Jiwu, H., "Edge adaptive image steganography based on LSB matching revisited", IEEE Transactions on Information Forensics and Security, Vol.5, no.2, pp.201-214, 2010.
[31] Yu, Y., Chang, C., Lin, I., "A new steganography method for color and grayscale image hiding", Computer Vision and Image Understanding, Vol.107, no.3, pp.183-194, 2007.
[32] Adale, D. A., "Hybrid Information security models: crypto-stego and stego-crypto systems", Thesis in Masters of Computer Science, Department of Systems and Computer Science, Howard University, 2011.
[33] Karthikeyan, B., Vaithiyanathan, V. , Thamotharan, B. , Gomathymeenakshi, M., Sruti, S., "LSB replacement steganography in an image using pseudo randomized key generation", Research Journal of Applied Sciences, Engineering and Technology, Vol.4, no.5, pp.491-494, 2012.
[34] El-Emam, N., "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science, Vol.3, no.4, pp.223-232, 2007.
[35] Gupta, S., Goyal, A., Bhushan, B., "Information hiding using least significant bit steganography and cryptography", I.J. Modern Education and Computer Science, Vol.6, pp.27-34, 2007.
[36] Kavitha, Kavita, K., Ashwini K., Dunghav, P., "Steganography using least significant bit algorithm", International Journal of Engineering Research and Applications, Vol.2, no.3, pp.338-341, 2012.
[37] Zainal N. & Wadi S.M., "Decomposition by binary codes-based speedy image encryption algorithm for multiple applications", IET Image Processing Vol.9, no.5, p.p. 413-423, 2015.