Applied Mathematical Sciences, Vol. 9, 2015, no. 48, 2381 - 2391
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2015.53219

Secured Patient Information Transmission Using Reversible Watermarking and DNA Encrytion for Medical Images

C. Vinoth Kumar

Departmentof ECE
SSN College of Engineering, Kalavakkam, India

V. Natarajan

Department of Instrumentation Engineering
MIT campus, Anna University, Chennai, India

P. Poonguzhali

Department of ECE
SSN College of Engineering, Kalavakkam, India

Abstract

Reversible Watermarking is the technique of embedding secret messages into a cover image and recovering both the embedded secret message and the cover image without any distortion. One of the high quality and popular reversible data hiding methods is Difference Expansion method. In this paper, Difference Pair Mapping (DPM) method is used to embed the message into the cover image. The DPM method is based on predicting the pixel values and hiding the secret data with arbitrary threshold. The simulation results show that the hiding capacity is increased in DPM method when compared to other Difference Expansion techniques. Further, in order to provide security, DNA based encryption algorithm is used to resist the statistical and exhaustive attacks over the image. The combined difference expansion and encryption algorithm provides high embedding capacity along with high security.

Keywords: Reversible Watermarking, Difference Pair Mapping, Gradient-Adjusted-Prediction, DNA Encryption

1 Introduction

Reversible watermarking is the process of hiding the data in the cover media like image, video audio, etc. In applications such as military, health care information management systems and medical images, the RDH technique is responsible for protecting both the image and the content. In reversible data hiding both secret message and cover media is recovered without any distortion. Authenticity is proved by means of watermark of the image which acts as a key. The reversible watermarking provides both authentication and tamper proofing for both cover image as and patient information. The basic requirements of reversible data hiding are embedding capacity and low distortion.Various RDH techniques have been proposed based on lossless compression [1-3], Difference expansion, Histogram modification, Prediction-error expansion and Integer transform. Ni et al. [7] proposed first histogram based RDH method utilizing peak and minimum points of pixel-intensity-histogram to embed data. Lee et al. [5] proposed difference histogram to embed more data. Lee et al.s method can be implemented by modifying the two-dimensional pixel-intensity-histogram according to injective mapping defined on pixel pairs which is known as Pixel-Pair-Mapping (PPM). Fallahpour [6] introduced a method by modifying the histogram of prediction-error in which the prediction-error-histogram is sharply distributed which guarantees an excellent embedding performance.

Difference expansion techniques by Tian [3] embeds the data by expanding the difference between the two neighbouring pixels of the pixel pairs. The redundant space in the image was explored to hide more data. More amounts of data can be embedded in cover media, with a considerable amount of side information, which indicates the locations of the hidden data. The existing Lee method [5] of difference expansion, groups two columns of pixel values in a cover image forming a pixel pair which is then used to create a difference image for the purpose of data embedding. Pixel Pair Mapping (PPM) is the another existing difference expansion method,which is modified version of Lee method. PPM method groups two columns of pixel values along both the direction (forward and backward) and creates redundant space for embedding data.

Most of reversible watermarking techniques concentrate more on hiding capacity and image quality. In this paper, both hiding capacity and security is also addressed. Image encryption along with reversible data hiding is used to improve the security. Kuldeep Singh et al [12] proposed a new method in Image encryption using chaotic maps and DNA addition operation where noise has a little effect on original image. Qiangzhang et al [13] proposed a new image encryption algorithm based on DNA sequence addition operation. DNA sequence matrix is obtained by encoding the original image and the DNA sequence matrix is divided into some equal blocks. DNA sequence addition operation is used to add these blocks. Then DNA sequence complement operation is performed for the result of added matrix by using two Logistic maps. The DNA sequence matrix is decoded to get the encrypted image. Qian Wang et al [30] proposed a new image algorithm based on DNA coding and chaos sequence where the location of pixels and pixel values are changed through the combination of chaos with DNA coding. Xu Shu-Jiang et al [14] proposed an image encryption method based on chaotic maps. By combining XOR operations and circular bit shift operation, the security of this encryption algorithm is enhanced effectively. Two chaotic maps are used in proposed algorithm. One chaotic map generates a binary stream for XOR operation, and the other generates random numbers which are used for circular bit shift operation. This algorithm has a high security and a good efficiency. Yun peng Zhang et al [15] proposed an Image Encryption scheme Based on Multiple Chaos System. The sub key sequences are generated from the chaotic maps which have certain relation to the plaintext, which enhances the security of the cryptosystem. The proposed system makes use DNA based encryption technique with Difference pair mapping method to improve the security and reversibility in medical images.

The section II gives overview of difference expansion method, pixel pair mapping method and difference pair mapping method. The section III provides information about DNA encryption. Section IV includes the proposed system. Section V contains the simulations and experimental results. Finally conclusion and future work is discussed.

2 Difference expansion method

In difference expansion technique difference between pixel pair is used to embed the data. The difference value is doubled and a bit is embedded either by expanding difference or by changing the LSB of difference value. So two categories of pixels are made which are expandable pixels and changeable pixels. The expandable or the changeable pixels are decided based on the threshold chosen. Location map is used to prevent overflow and underflow problem. Lee et al.s method of difference expansion is implemented by modifying the two-dimensional pixel-intensity-histogram according to a Pixel Pair Mapping

(PPM). Pixel Pair Mapping (PPM) is the modified version of existing Lee method,which groups two columns of pixel values along both the direction (forward and backward) and creates redundant space for the data to be embedded. The modified PPM method involves combination of existing PPM method and the modified Lee method by grouping any number of columns thereby creating more redundant space along both the directions (forward and backward). The number of columns to be grouped is defined by the user. The pixel pair formed by grouping any number of columns is always one less than the number of columns grouped. The redundant space for the purpose of data embedding created by the proposed method is more when compared with the existing methods.

2.1 Difference pair mapping (DPM) method

Difference Pair Mapping (DPM) is also an injective method utilizing the values of difference pairs. DPM method is implemented along both the directions (forward and backward) is an extended version of DPM. In bi-directional DPM the difference values for pixels is obtained by making use of the prediction values of pixel-pairs. The prediction values are obtained along both the direction. Consider a pixel-pair (x, y), in forward direction the prediction value of y is used for computing the difference value and in reverse direction the prediction value of x is used for computing the difference value. By utilizing the prediction values and the arbitrary threshold value, DPM method along both the direction (forward and backward) aims to increase the embedding performance.

In order to compute the prediction value of x, the Gradient-Adjusted-Prediction (GAP) is used for an accurate estimation which is used in adaptive embedding technique. Since most of the medical images contain darker areas more than lighter areas, the space for embedding the data is usually is less in medical images. By making use of the prediction values the DPM method selects smooth pixels for the purpose of data embedding. The DPM technique carried out in both forward and reverse direction produces better embedding performance (Hiding capacity) than forward direction [11]. The prediction values computed along both the direction makes the embedding process secure by making the data to be known only for the intended receiver.

Table 1: Context of (x, y)

i/j	j	j+1	j+2	j+3
i	x	y	$v1$	$v2$
i+1	$v3$	$v4$	$v5$	$v6$
i+2	$v7$	$v8$	$v9$	$v10$

For each pixel-pair (*x, y*), the prediction of x to get z is computed using GAP predictor as in [15] and [24]:

$$z = \begin{cases} u & \text{if } 80 < (dv - dh) \\ (v1+u)/2 & \text{if } (32 < (dv - dh) <= 80) \\ (v1+3u)/4 & \text{if } (8 < (dv - dh) <= 32) \\ u & \text{if } (-8 < (dv - dh) <= 8) \\ (v4+3u)/4 & \text{if } (-32 <= (dv - dh) < -8) \\ (v4+3u)/2 & \text{if } (-80 <= (dv - dh) < -32) \\ v4 & \text{if } (dv - dh) < -80) \end{cases} \tag{2.1}$$

where $v1$,..$v7$,$v8$ are neighbouring pixels of (*x, y*), dv=|$v1$-$v5$|+ |$v3$-$v7$| + |$v4$-$v8$| and dh=|$v1$-$v2$| + |$v3$-$v4$| + |$v4$-$v5$| represents the vertical and horizontal gradients, and u=($v1$ + $v4$)/2 + ($v3$-$v5$)/4. The predicted value of y (z) should be rounded to the nearest integer if it is not an integer. For each pixel-pair with a noisy-level less than a threshold T, the difference-pair (D1, D2) is computed. The data embedding and data extraction procedure is similar to Lee et al PPM method. The difference image D1 =x-$y$and D2 =y-z are calculated, which are used to embed the data into the cover image.

Algorithm for embedding and extraction:

Step 1: Consider an image of size m x n.
Step 2: Difference image is computed using the formula
D1(i,(g-1)*j-(g-1-k)) = I(i,g*j-(g-1-k)))-(I(i,g*j-(g-1))) (2.2)
D2(i,(g-1)*j-(g-1-k)) = I(i,g*j-(g-1)))-(y(i,g*j-(g-1))) (2.3)
The size of the difference image D1 and D2 are m x (n/g) where g is the number of columns being grouped and k is the number of pixel pairs formed after grouping of columns.
Step 3: The marked value of the cover pixel pair can be calculated as given in Table2.
Step 4: Embedded data bit b can be extracted from the marked pixel pair based on the conditions (d_1^m,d_2^m) given in Table3, where d_1^m = x^m - y^m and d_2^m= y^m - z. For reverse direction, data embedding and extraction from step 2 to step 4 is carried over in the reverse direction by predicting x pixel values.

3 DNA based encryption

Encryption techniques are used to protect the images from the threat during the process of transmission of digital image over internet. DNA based encryption schemes are more resistive to statistical and differential attacks. So DNA based encryption is used to enhance the security of reversible data hiding. A DNA sequence contains

Table 2: Conditions for embedding data

Conditions(d_1,d_2)	**Marked Value**
d_1= -1 and $d_2 > 0$	(x+b, y)
d_1 = -1 and $d_2 < 0$	(x-b, y)
$d_1 = 0$ and $d_2 \geqslant 0$ $d_1 < 0$ and $d_2 = 0$	(x, y+b)
$d_1 = 0$ and $d_2 < 0$ $d_1 > 0$ and $d_2 = 0$ $d_1 = 1$ and d_2 = -1	(x, y-b)
$d_1 > 1$ and $d_2 > 0$	(x+1, y)
$d_1 <$ -1 and $d_2 < 0$	(x-1, y)
$d_1 < 0$ and $d_2 > 0$	(x, y+1)
$d_1 > 1$ and $d_2 < 0$ $d_1 = 1$ and $d_2 <$ -1	(x, y-1)

Table 3: Conditions for extracting data

Conditions on (d_1^m, d_2^m)	**Extracted bit b**	**Recovered value**
$d_1^m \in \{1,2\}$ and $d_2^m > 0$	d_1^m - 1	(x^m b, y^m)
$d_1^m \in \{-1,-2\}$ and $d_2^m < 0$	-1 - d_1^m	(x^m + b, y^m)
($d_1^m = 0$ and $d_2^m \geqslant 0$)or (d_1^m = -1 and $d_2^m \geqslant 1$)	- d_1^m	(x^m , y^m - b)
($d_1^m < 0$ and $d_2^m = 0$) or ($d_1^m <$ -1 and $d_2^m = 1$)	d_2^m	(x^m , y^m - b)
($d_1^m = 0$ and $d_2^m < 0$) or ($d_1^m = 1$ and $d_2^m <$ -1)	d_1^m	(x^m , y^m + b)
($d_1^m > 0$ and $d_2^m = 0$) or ($d_1^m > 1$ and d_2^m = -1)	- d_2^m	(x^m , y^m + b)
($d_1^m = 1$ and d_2^m = -1)or ($d_1^m = 2$ and d_2^m = -2)	d_1^m - 1	(x^m , y^m + b)
$d_1^m > 2$ and $d_2^m > 0$	No embedded data	(x^m 1, y^m)
$d_1^m <$ -2 and $d_2^m < 0$	No embedded data	(x^m + 1, y^m)
$d_1^m <$ -1 and $d_2^m > 1$	No embedded data	(x^m , y^m - 1)
$d_1^m > 2$ and $d_2^m <$ -1 $d_1^m = 2$ and $d_2^m <$ -2	No embedded data	(x^m , y^m + 1)

four nucleic acid bases A(adenine), C(cytosine), G (guanine), T(thymine), where A and T is complement, G and C is complement. In this method, 00, 01, 10, 11 is used to denote C, A, T, G, respectively. For 8 bit grey images, each pixel can be expressed as a DNA sequence whose length is 4.Addition and subtraction operation for DNA sequences are performed using addition and subtraction table described in Qiang method[13]. The important step in encryption is generation of secret keys.

The secret keys are generated based on Qiang method[13]. DNA sequence matrix is obtained by encoding the original image. The DNA sequence matrix is divided into equal blocks. DNA sequence addition operation is used to add these blocks. Then DNA sequence complement operation is performed for the result of added matrix by using two Logistic maps. By decoding the complement DNA sequence matrix the encrypted image is generated.

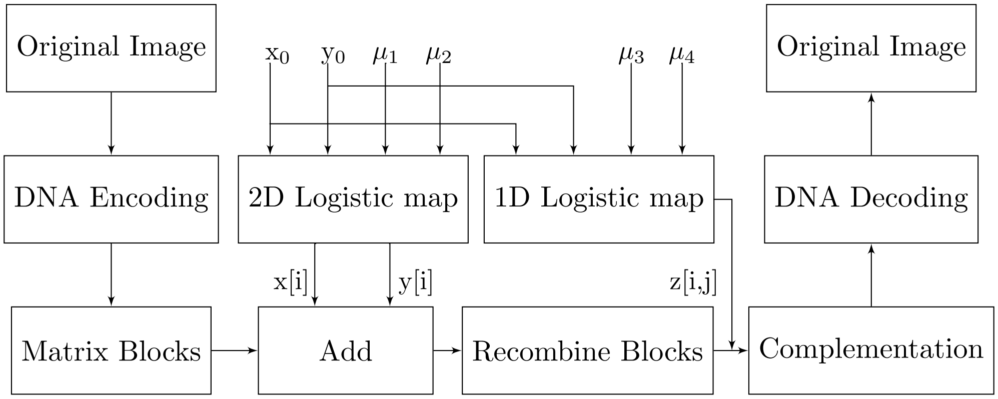


Fig.1 Block diagram of Image Encryption

Step 1: Convert each pixel in the original image into binary and then carry out DNA encoding and obtain a coding matrix A$_b$ of mx(nx4)from an original image A of mxn.
Step 2: Divide A$_b$ into some equal blocks, A$_{b1}$ {i, j}, i=1,2.....m/4, j=1, 2 ...n, where size of each block is 4x4.
Step 3: Generate two chaotic sequence X={x$_1$, x$_2$ ...x$_{m/4}$}, Y={y$_1$, y$_2$......y$_n$} through 2D logistic map under the condition that initial values are x$_0$,y$_0$ and system parameters are μ_1,μ_2.
Step 4: Reconstruct X and Y into row and column matrix respectively. Do multiply operation on both to get a chaotic matrix K and then convert it into a binary matrix. Using DNA encoding rule convert it into a DNA encoded Chaotic matrix K. Divide K into small cells K{i, j} each of size 4x4.
Step 5: Add A$_{b1}${i, j} and K{i, j} using DNA addition to obtain added cell B{i, j}.
Step 6: Recombine these B {i, j} to get new sequence matrix C.
Step 7: Again two chaotic sequences Z$_1$ and Z$_2$ are produced using whose length is m and nx4.
Step 8: Reconstruct Z$_1$ and Z$_2$ into two matrix Z$_1$ (m, 1) and Z$_2$ (1, nx4). Do multiply operation to get Z matrix whose length is (m, nx4).
Step 9: Map the values of z into (0,1) by mod(Z,1).Get binary sequence matrix using the following threshold function.

$$F(x) = \begin{cases} 0 & \text{if } 0 < z(i,j) <= 0.5 \\ 1 & \text{if } 0.5 < z(i,j) <= 1 \end{cases} \tag{3.1}$$

Step 10: If Z (i, j) =1, C (i, j) is complemented. Otherwise it is unchanged. Hence a complemented matrix P is formed.
Step 11: Carry out the inverse process of step1 for P to get the encrypted Image E.
Step 12: Decryption is done by processing from step11 to step1, where DNA addition is replaced by DNA subtraction operation. Receiver will obtain the secret key from the sender through the secure channel.

4 Proposed System

This work uses both Difference pair Pixel Mapping and DNA encryption scheme to transmit patient information. The Fig.2 shows the proposed methodology, where DPM is used for embedding the secret information into the image and DNA encryption used for providing the security to the stego-image. The medical image is analysed and estimated using GAP method. The secret information is embedded into the medical image based on the difference between the input image and the predicted image, as explained in section II. Then, the stego-image is encrypted using DNA encryption algorithm as described in the section III.

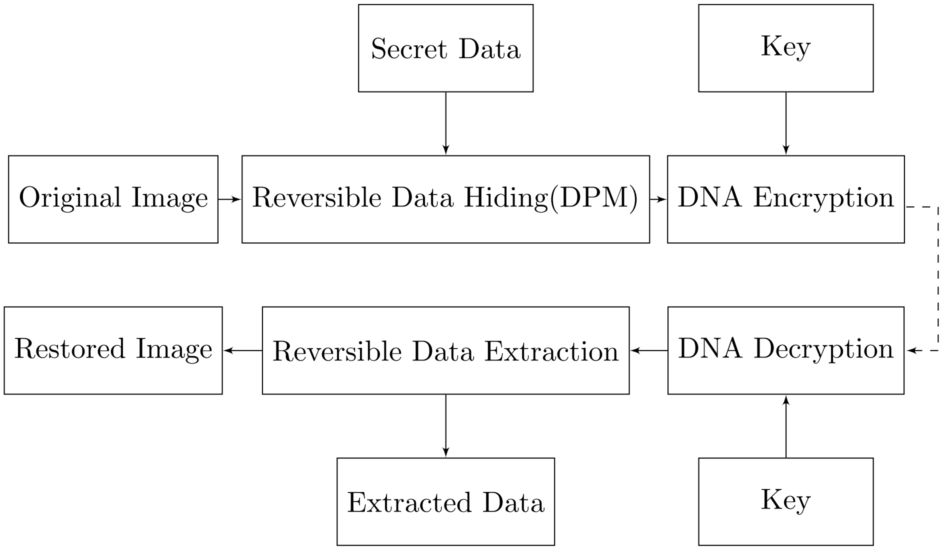
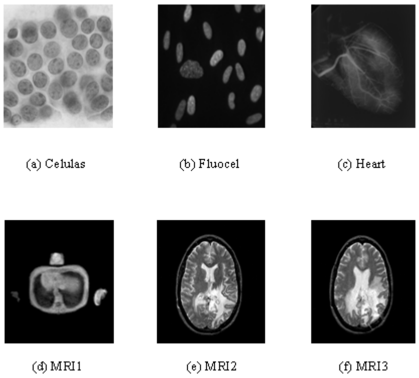


Fig.2 Block diagram of proposed system

The encrypted stego image is transmitted from place to another, where the secret information and the original image are restored using DNA decryption algorithm and inverse DPM method. In the proposed approach, the GAP prediction method and DNA encryption key are known only to the sender and the receiver. Hence, the medical image and patient information are securely shared between two users. The location map, which shows the position of overflow and underflow error, is also embedded into the stego image before DNA encryption.

5 Simulation results

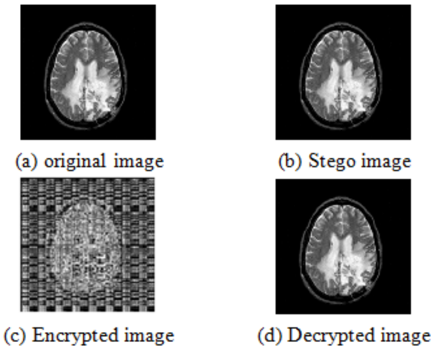
The DNA encryption based reversible watermarking is applied for six gray scale medical images of size 256 x 256 which are shown in Fig.3. The proposed methodology is compared with Lees PPM and modified PPM method in terms of embedding capacity. Table 4 reveals that the hiding capacity is improved in the proposed approach when compared to the other methods. The threshold determines the pixel-pair selection for data embedding. By varying the threshold, the embedding capacity and the stego image quality varies.



(a) Celulas (b) Fluocel (c) Heart

(d) MRI1 (e) MRI2 (f) MRI3

Fig.3 Test Images



(a) original image (b) Stego image

(c) Encrypted image (d) Decrypted image

Fig.4 Simulation results

The experimental results for the above medical images are produced with the threshold T=120, for maximum embedding capacity. The threshold varies with the energy possessed by the medical image. The input medical image and the patient information are restored without any distortion using DNA decryption algorithm and inverse DPM method. The simulation result is shown in fig.4. The security analysis of the DNA encryption algorithm is beyond the scope of this paper and it will be investigated in the future work.

Table 4: Comparison for hiding capacity between Lee method, PPM method and DPM method

Images 256x256	Lee Method	PPM	DPM
Celulas	3378	4469	5565
Fluocel	4457	5573	6513
Heart	4159	5462	6063
MRI1	1389	2483	2794
MRI2	2061	3404	3654
MRI3	2239	3645	4285

6 Conclusion

In this paper, DPM and DNA encryption based reversible watermarking for medical images is implemented. The scheme does not require any data compression to maintain the visual quality of the watermarking image. The study shows that the DPM method provides high embedding capacity when compared to other Difference Expansion Techniques. The pixel-pair selection strategy is an important parameter to improve the embedding capacity. The pixel-pair selection is based on the threshold which depends on energy of the cover medical image. This paper discusses only the Gradient Adjusted Prediction in DPM method. An investigation may be done with different threshold value with several other prediction schemes and encryption methods.

References

[1] M. U. Celik, E. Saber, G. Sharmaand and A. M. Tekalp, Lossless generalized-LSB data embedding,IEEE Trans. Image Process., Vol. 14,no.**2**,pp. 253−266, Feb. 2005. http://dx.doi.org/10.1109/tip.2004.840686

[2] C. C. Chang, W. L. Tai and C. M. Yeh, Reversible data hiding based on histogram modification of pixel differences, IEEE Trans. Circuits Syst. Video Technol., vol. 19, no.**6**, pp. 906−910, Jun. 2009. http://dx.doi.org/10.1109/tcsvt.2009.2017409

[3] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol., vol. 13, no.**8**, pp. 890−896, Aug. 2003. http://dx.doi.org/10.1109/tcsvt.2003.815962

[4] A. M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. Image Process., vol.13, no.**8**, pp. 1147−1156, Aug. 2004. http://dx.doi.org/10.1109/tip.2004.828418

[5] Y. S. Ho, S. K. Lee and Y. H. Suh, Reversible image authentication based on watermarking, in Proc. IEEE ICME, 2006, pp. 1321−1324. http://dx.doi.org/10.1109/icme.2006.262782

[6] M. Fallahpour, Reversible image data hiding based on gradient adjusted prediction, IEICE Electron. Express, vol. 5, no.**20**, pp.870−876, Oct. 2008. http://dx.doi.org/10.1587/elex.5.870

[7] N. Ansari, Z.Ni, Y.Q. Shi and W. Su, Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol., vol. 16, no.**3**, pp. 354−362, Mar. 2006. http://dx.doi.org/10.1109/tcsvt.2006.869964

[8] T. S. Chen, W. Hong and C. W. Shiu, Reversible data hiding for high quality images using modification of prediction errors, J. Syst.Software, vol. 82, no.**11**, pp. 1833−1842, Nov. 2009. http://dx.doi.org/10.1016/j.jss.2009.05.051

[9] X. Li, B. Yang and T. Zeng, Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process., vol. 20, no.**12**, pp. 3524−3533, Dec. 2011. http://dx.doi.org/10.1109/tip.2011.2150233

[10] Y. Hu, H. K. Lee and J. Li, DE-based reversible data hiding with improved overflow location map, IEEE Trans. Circuits Syst. Video Technol., vol. 19, no.**2**, pp. 250−260, Feb. 2009. http://dx.doi.org/10.1109/tcsvt.2008.2009252

[11] Bin Yang, Weiming Zhang, Xiaolong Li and Xinlu Gui, A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification, IEEE Trans. Inf. Forensics Security, vol. 8, no.**7**, pp. 1091−1100, Jul. 2013. http://dx.doi.org/10.1109/tifs.2013.2261062

[12] Komalpreet kaur and Kuldeep singh, Image encryption using chaotic maps and DNA addition operation and noise effects on it, International Journal of Computer Application, Vol.23, pp.17,2011. http://dx.doi.org/10.5120/2892-3779

[13] Ling Guo, Qiangzhang, Xiang Lian Xue, Xia Opeg Wei, An image encryption algorithm based on DNA sequence addition operation, IEEE Fourth International Conference on Bio-Inspired Computing, Vol. 26, pp. 1−5.2009. http://dx.doi.org/10.1109/bicta.2009.5338151

[14] Tian Min, Xu Shu-Jiang, Wang Ying-Long and Wang Ji-Zhi, A Novel Image Encryption Scheme Based on Chaotic Maps, ICSP 9thInternational Conference on Signal Processing,Vol.10,pp.1014−1018,2008. http://dx.doi.org/10.1109/icosp.2008.4697300

[15] Cai Xiaobin, Fei Zuo, Yunpeng Zhang and ZhengjunZhai, A New Image Encryption Algorithm Based on Multiple Chaos System, International Symposium on Electronic Commerce and Security, pp. 347−350,2008. http://dx.doi.org/10.1109/isecs.2008.142

Received: December 15, 2014; Published: March 21, 2015