American International Journal of Research in Science, Technology, Engineering & Mathematics

Available online at http://www.iasir.net

ISSN (Print): 2328-3491, ISSN (Online): 2328-3580, ISSN (CD-ROM): 2328-3629

AIJRSTEM is a refereed, indexed, peer-reviewed, multidisciplinary and open access journal published by
International Association of Scientific Innovation and Research (IASIR), USA
(An Association Unifying the Sciences, Engineering, and Applied Research)

Dual Layer Image Scrambling Method Using Improved Arnold Transform

[1]Gyan Vardhan Artist, [2]Dr. Mahesh Kumar Porwal
[1]M.Tech, Digital Communication, [2] Professor, ECE Department
Shrinathji Institute of Tech & Engg, Nathdwara, Rajsamand, Rajasthan, INDIA

***Abstract**: In this paper various version of image scrambling based on Arnold transform are discussed and new method, which is an extension of improved Arnold Transform is proposed, and then compared those method statistically and by figures, experimental result clearly revels that proposed method gives better result then previous versions of Arnold Transform*

***Keywords**: Arnold transform, block location scrambling, multi area scrambling, improved arnold transform*

I. Introduction

With the rapid development of computer network and multimedia technology, security problem of digital images has been highlighted, therefore image encryption technology has become vast topic of research [9]. Image encryption converts true image into meaningless image [4]. There are many algorithms about image scrambling such as orthogonal latin square, affine transform, magic square, baker transformation, Fibonacci transformation and so on. These methods have different visual effects but they have certain limitations like there parameters are small hence ability of encryption is small which use for simple data encryption [7]. Arnold transform is widely used in image scrambling since it is periodic in nature. It is mainly encryption and decryption tool. It disturbs image auto correlation and creates chaotic random image, which makes it impossible to get original image without using improved Arnold transform. Arnold transform is named after 'VLADIMIR ARNOLD' and he demonstrate its effect on cat map, hence it is also known as "ARNOLD CAT MAP" [5]. It is basically a tool of changing one matrix into another matrix. It is very simple and easy to implement. It is point to point transform which shuffles each pixel value in an image.

II. Arnold Transform

A. *Traditional Arnold transform [5]*

Arnold transform is given by :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N \tag{1}$$

where

x ,y = original image co-ordinate
x', y' = transform image co-ordinate

demerits of above conventional Arnold transform is that the all four transform parameters or coefficients are fixed in nature so if somehow any one can identify that conventional Arnold transform is used to scramble the image, by using fixed value of those coefficient , he can easily descramble the image.

B. *Block location scrambling algorithm of digital image based on Arnold transform [9]*

It performs similar Operation to Arnold transform except its matrix coefficients are different from traditional Arnold transform.

The transform algorithm for above proposed algorithm is given below:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} modN \tag{2}$$

QI DAONG-XU has proved that for a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ when elements satisfying the criteria that ad-bc = 1 [9]. Its transformation coefficients can be used as scrambling transformation. Demerits of above algorithm is that out of four matrix coefficients only two coefficient are unknown so we have a limited choice to choose different matrix coefficients i.e. or simply 2. Secondly its first matrix coefficients i.e. are still fixed to one or unity.

C. *Improved Arnold Transform or IAT [5]:*

This transform is proposed in 2010 by MA DING & FAN JING .Transform equation for IAT is given as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + K \begin{pmatrix} N \\ N \end{pmatrix} modN \quad (3)$$

$$a_{00} \times a_{11} + a_{01} \times a_{10} = \pm 1 \quad (4)$$

$$K{=}max[ABS(a_{00}), ABS(a_{11}), ABS(a_{10}), ABS(a_{01})] \quad (5)$$

$$\text{A}{=}\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \quad (6)$$

Where

Eq. 3 = matrix for Improved Arnold Transform or IAT

Eq. 6 = transformation matrix coefficient, which can be any

Matrix or could be conventional matrix$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

When transform matrix choose different coefficients, K is having maximum value from transform matrix coefficient, which ensures that transformed parameters are to be not negative. And hence we get unique inverse matrix, when this matrix is nonsingular in nature that means the determinant of that matrix is non-zero which is shown below:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} + K \begin{pmatrix} N \\ N \end{pmatrix} modN \quad (7)$$

D. *Advantage of improved Arnold transform over above variants of Arnold Transform:*

(1) In improved Arnold transform, various sets of matrix coefficients can be used while conventional Arnold matrix uses fix set of matrix coefficients.

(2) In IAT all four matrix coefficients are different and we have a lot of choice to choose them but in Block location scrambling algorithm first parameter (a_{11}) is fixed to unity and we have only 2 choice to select rest three coefficients.

(3) Scrambling factor that used to calculate difference among true real image and transformed image should be as high as possible so if we somehow able to increase scrambling factor then it is difficult for the attacker to get original content of an image. That is what we did in this proposed algorithm.

E. *Proposed extension of improved Arnold transform :*

Above concept is based on IAT, in which scrambling ratio is improved significantly by dividing an image into either four or sixteen sub-images. Then apply improved Arnold transform on each sub-image. By doing so size of an original image is changed..

When an image is divided into

(1) Four sub-images = size of each sub-image is 128*128

(2) Sixteen sub-images = size of each sub-image is 64*64

The greatest advantage of proposed algorithm is that different sub-images can be sent at different frequency and via different route to its destination. At the destination side true image can be reconstructed by knowing:

(a) Exact transform matrix coefficients, which was used to scramble an image.

(b) Correct size of an image

(c) Frequency for particular size of an image because frequency depends on size of an image.

Frequency for size as shown in table below [5]:

Size of an image	32	64	100	125	128	256	512
Image frequency	24	48	150	250	96	192	384

(d) Meaningless sub-images must be put at proper place so that random meaningless image can form meaning full content of an image.

So it is very difficult for the attacker to get original image because:

(1) Instead of sending complete image, we are sending sub-images, which can be sent at same or different frequency.

(2) Sub-images can be sent either in same order or in different order so it looks like a random image until sub-images are rearranged in a proper way.

Hence by doing so security of improved Arnold transform is greatly increased since scrambling ratio is increased.

III. Calculation for scrambling ratio

Steps to be used to calculate scrambling ratio [5]:

(1) Divide the whole image into block size of 4*4.
(2) Compute mean and variance for each block.
(3) Compute image mean square signal to noise or SNR ratio.
(4) Put above calculate value in the scrambling ratio formula.

The formula to calculate mean, variance and SNR are shown below:

$$\mu = \frac{1}{4\times4}\sum_{x=1}^{4}\sum_{y=1}^{4} I(x,y) \tag{8}$$

$$D=\sum_{B=1}^{L}\frac{1}{4\times4}\sum_{x=1}^{4}\sum_{y=1}^{4}(I(x,y)-\mu)^2 \tag{9}$$

$$SNR=\frac{\sum_{x=1}^{N}\sum_{y=1}^{N}(I(x,y))^2}{\sum_{x=1}^{N}\sum_{y=1}^{N}(I(x,y)-I'(x,y))^2} \tag{10}$$

By Defining the image scrambling ratio, which is given below:

$$\boldsymbol{n} = \frac{D'}{D}\times\frac{1}{SNR} \tag{11}$$

Where
D = variance before scrambling of an image
D’= variance after scrambling of an image
I = true image and I’ = scrambled image
N = order of an Image

Ratio of image variance is increased when difference between each pixel gray value and mean is increased. The frequency at which an image cannot be reconstructed, at those frequency value of SNR is decreased and vice-versa is also true. Because from SNR eq. it is clear that SNR will decreased when denominator is increased that means difference between original image and scrambled image is increased and hence scrambling ratio is increased. While the frequency at which image is reconstructed properly, value of SNR is increased i.e. difference between true original image and scrambled image is decreased, since image is restored properly, this is the only and unique frequency at which image is recovered.

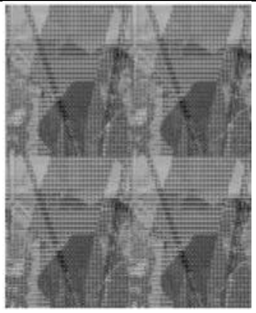
IV. Simulation result

The comparison of above discussed algorithm in tabular form and in the form of an image.

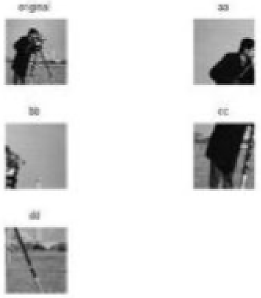
A. ***For cameraman.tif image:***

frequency	AT	IAT	IAT	
f			4 sub-image	16 sub-image
5	2.4842	2.6088	2.7713	2.7788
50	2.8769	2.9079	3.0199	3.0298
100	2.8514	3.0296	2.9926	3.0709
192	0	2.0777	1.2209	1.2207

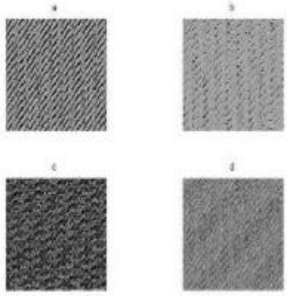
(1) Original Image


(2) Recovered from AT

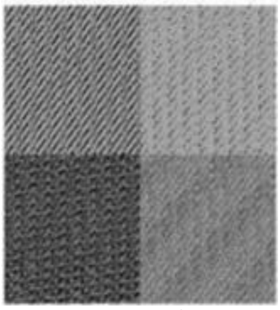
(3) Recovered from IAT

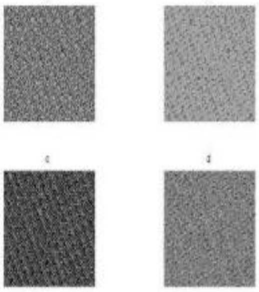


(4) true & 4 sub-images

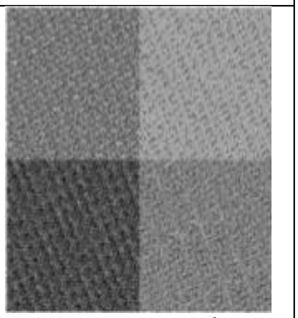


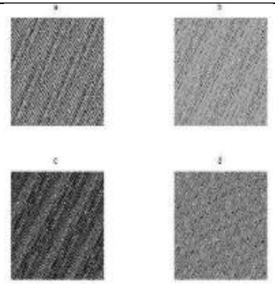
(5) 4 sub-images at f = 5

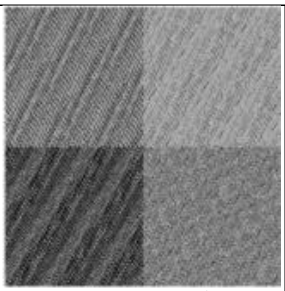

(6) recover image at f =5



(7) 4 sub-images at f = 50

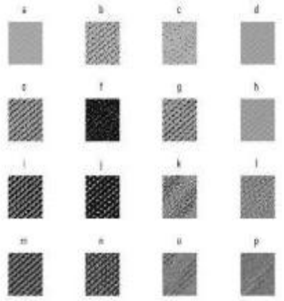

(8) recover image at f = 5

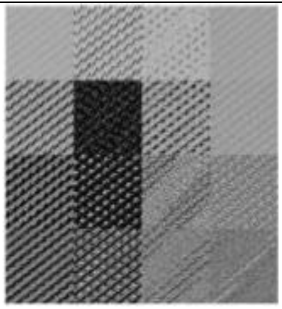

(9) sub-images at f = 100

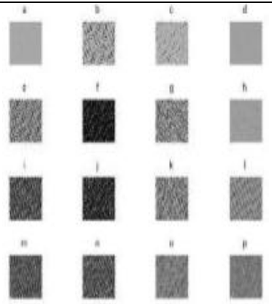

(10) recover image at f= 100

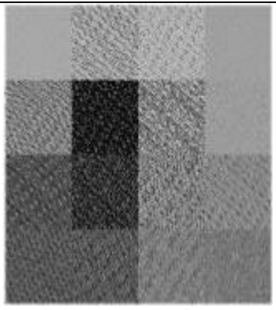
(11) sub-images at f=192

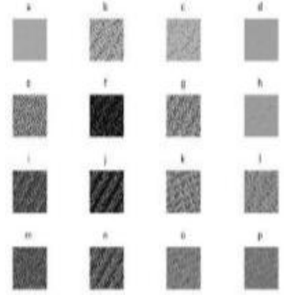
(12) recovery at f = 192

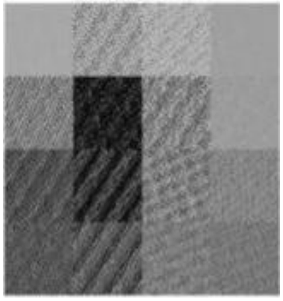

(13)16 sub-image at f = 5

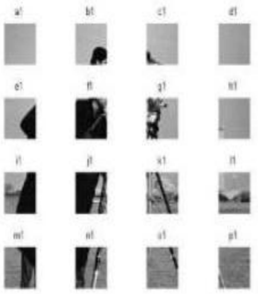

(14) recovery at f=5


(15) 16 sub-images at f=50


(16) recovery at f = 50


(17) 16 sub-images at f = 100


(18) recovery at f = 100


(19) 16 sub-images at f = 192

(20) recovery at f = 192

B. *for Lena.jpg image*

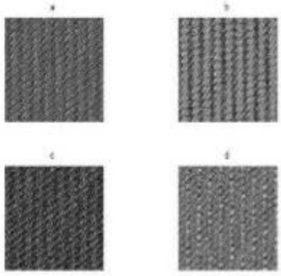
frequency	AT	IAT	IAT	
f			4 sub-image	16 sub-images
5	2.1107	2.1651	2.1891	2.2192
50	2.3396	2.3539	2.3815	2.3832
100	2.255	2.274	2.2974	2.3971
192	0	0.6277	0.62	0.6277

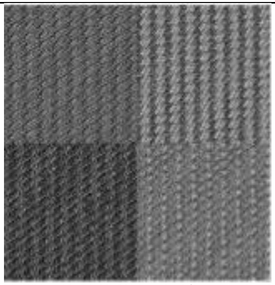
(21) original image

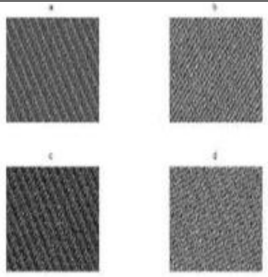
(22) recovery from AT

(23) recover from IAT

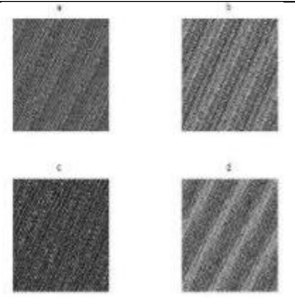
(24) true & 4 sub images

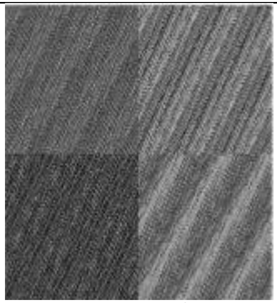

(25) 4 sub-images at f = 5


(26) recovery at f = 5


(27) sub-images at f = 50

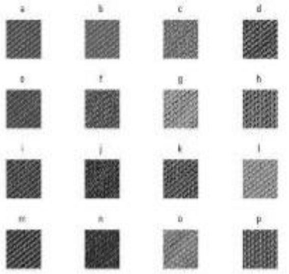
(28) recovery at f = 50

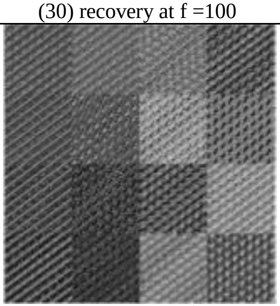

(29) sub-images at f = 100

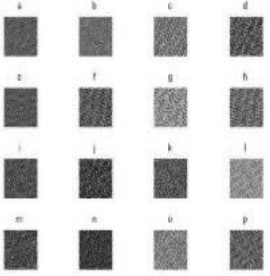

(30) recovery at f =100

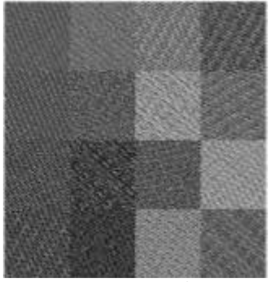
(31) 4 sub-images at f = 192

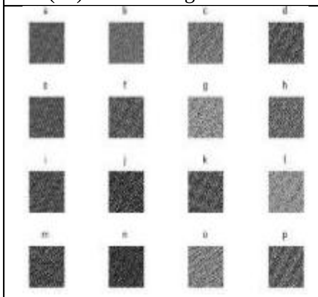
(32) recovery at f = 192

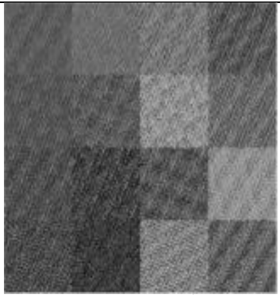

(33) 16 sub-images at f = 5


(34) recovery at f = 5


(35) 16 sub-images at f = 50


(36) recovery at f =50


(37) sub-images at f = 100


(38) recovery at f = 100

(39) sub-images at f = 192

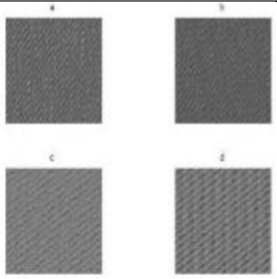
(40) recovery at f = 192

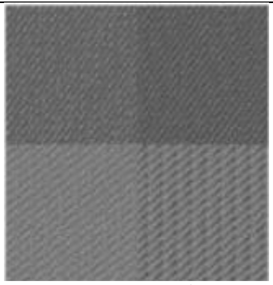
C. *for pout image*

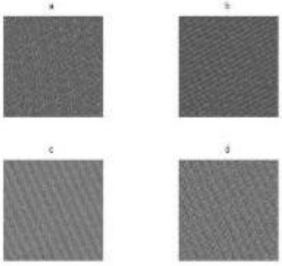
frequency	AT	IAT	IAT	
f			4 sub-images	16 sub-images
5	0.972	0.9889	1.0065	1.043
50	0.9942	1.027	1.975	1.9903
100	1.0361	1.227	1.9002	1.9303
192	0	0.4998	0.7665	0.7655

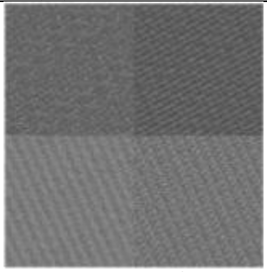
(41) true image

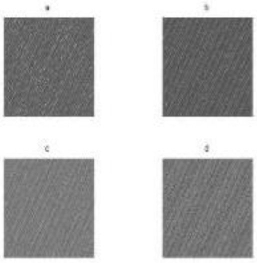
(42) recover from IAT

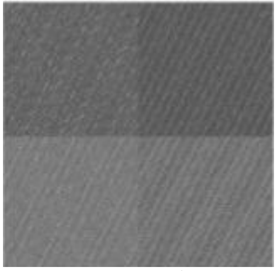

(43) 4 sub-images at f = 5

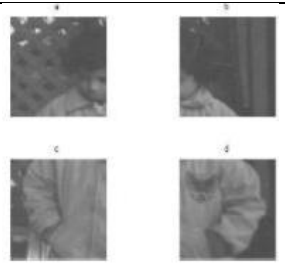

(44) recovery at f = 5

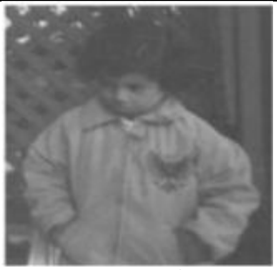

(45) 4 sub-images at f = 50

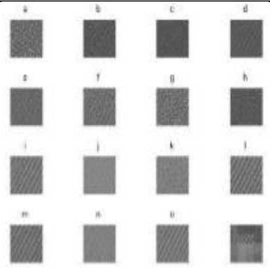

(46) recovery at f = 50

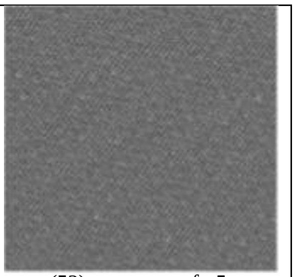

(47) 4 sub-images at f = 100

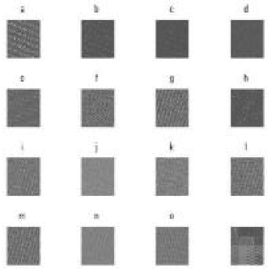

(48) recovery at f = 100

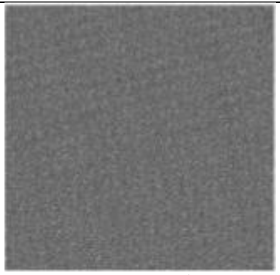

(49) 4 sub-images at f = 192

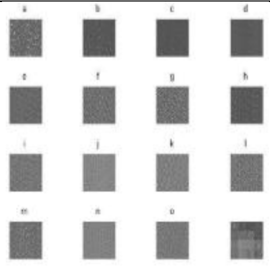

(50) recovery at f = 192

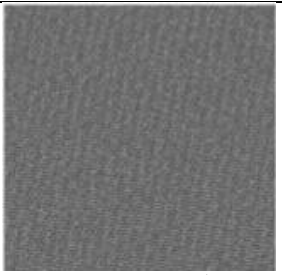

(51) 16 sub-images at f = 5

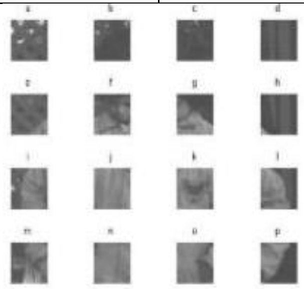

(52) recovery at f =5

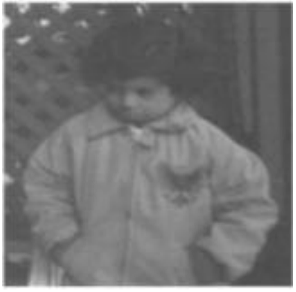

(53) 16 sub-images at f = 50


(54) recovery at f = 50


(55) 16 sub-images at f = 100


(57) 16 sub-images at f = 192


(57) 16 sub-images at f = 192


(58) recovery at f = 192

V. Remarks

(1) Image no. 2 and 22 give result from AT (Arnold Transform).

(2) Image no. 3, 23, and 42 give result from IAT (Improved Arnold Transform).

(3) Except image no. 2, 3, 22, 23, 42 give result from proposed AT (Arnold Transform).

(4) In this paper

- **(a)** f = frequency of Arnold Transform
- **(b)** AT = Arnold Transform
- **(c)** IAT = Improved Arnold Transform

VI. Conclusion

A new image scrambling concept is proposed in my paper. To encrypt an image with the help of image scrambling method, security of an image is improved by even better encryption method. That's what is done in this paper by using multi area scrambling concept [1] by choosing various transform coefficients, which creates dilemma for the attacker & hence leads to difficulty in deciphering the image since we are not using unique transform coefficients [1]. Statistical results and image shows that extended proposed algorithm is more efficient & hence can be used as digital image information hiding tool i.e. for watermarks. For different attacks it also shows excellent robust effect which does not affect original quality of an image hence can also be used in medical image processing. Hence above proposed method is extensively used because of its simple mathematical structure.

References

[1] Min Li^1 , Ting Liang2, Yu-Jie He^3. "Arnold Transform Based Image Scrambling Method". 3rd International conference on Multimedia Technology (ICMT 2013). Atlantis press pp. 1309-1316

[2] Veena V K, Jyothish Lal G, Vishnu Prabhu S, Sachin Kumar S, Soman K P. "A Robust Watermarking method based on Compressed Sensing and Arnold scrambling" 2012 IEEE . pp. 105-108.

[3] Jingbing Li, Mengxing Huang, Huaiqiang Zhang, Chunhua Dong, Yong Bai. "The Medical Images Watermarking Using DWT and Arnold". IEEE 2012, pp. 27-31.

[4] Zhenjun Tang and Xianquan Zhang. "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies". JOURNAL OF MULTIMEDIA, VOL. 6, NO. 2, APRIL 2011 Academy Publisher. pp. 202-206.

[5] Ma Ding, Fan Jing, "Digital Image Encryption Algorithm Based on Improved Arnold Transform". International Forum on Information Technology and Applications 2010 IEEE . pp. 174-176.

[6] Mingju Chen, Xingbo sun. "A Digital Image Watermarking of Self Recovery Base On the SPIHT Algorithm". 2nd International Conference on Signal processing System(ICSPS) 2010 IEEE. pp. 621-624.

[7] Lingling Wu, Weitao Deng, Jianwei Zhang, Dongyan He. "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm" . The 1st International Conference on Information Science and Engineering (ICISE) 2009 IEEE . pp. 1164-1167

[8] Zhang Yanqun, Wang Qianping. “A New Scrambling Method Based on Arnold and Fermat Number Transformation”. International Conference on Environmental Science and Information Application Technology 2009 IEEE. pp. 624-628.

[9] Zhenwei Shang, Honge Ren, Jian Zhang. “A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation” .the 9th International Conference for Young Computer Scientists 2008 IEEE. pp. 2942-2947.

[10] Chaokun Wang, Jianmin Wang, Ming Zhou, Guisheng Chen . “ATBaM: An Arnold Transform Based Method onWatermarking Relational Data” . International Conference on Multimedia and Ubiquitous Engineering 2008 IEEE. Pp. 263-270.