Fibonacci Based Text Hiding Using Image Cryptography

Manoj Mukherjee and Debabrata Samanta
Department of MCA, Acharya Institute of Technology, Bangalore, India
Email: manoj.mukherjee@ymail.com, debabrata.samanta369@gmail.com

***Abstract*—In digital word security is a most important issue and data hiding with image cryptography is one of the possible ways to ensure the security of the important message from outer world. In this paper we proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image.**

***Index Terms*—security, image cryptography, encryption technique, Fibonacci series, image encryption, secret key.**

I. Introduction

Security is a most important issue in communication and encryption is one of the ways to ensure security of the communicated message. Encoding is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decoding is the reverse of encoding; it is the transformation of encrypted data back into some intelligible form. Cryptography is popularly known as the study of encoding and decoding private massages. In cryptography, encryption processes are used in transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. The reverse process is referred to as decryption [1].

Steganography, which literally means "covered writing", Steganography is the more conservative technology to hide any secret information within an image. Steganography [2]. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in their Computer science and other related fields: they are used to protect e-mail messages, credit card information and etc. Steganography [3].Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in their Computer science and other related fields: they are used to protect e-mail messages, credit card information and etc. The proposed solution is to use image cryptography for disguising encrypted or normal textual information. This is a hybrid technique that inherits features from steganography and cryptography. Data hiding is a method used for hide information within computer code. By hiding the data, it's much harder to crack the code, because the data will appear invisible to the objects and the hacker.

A. Image Processing

It generally refers to processing of a two-dimensional picture by a digital computer.A digital image is a representation of a two-dimensional image as a finite set of digital values, called picture elements or pixels.Pixel values typically represent gray levels, colours, heights, opacities etc [18]. Then the image processing focuses on two major tasks

- Improvement of pictorial information for human interpretation
- Processing of image data for storage, transmission and representation for autonomous machine perception. Where image processing ends and fields such as image analysis and computer vision start. Our proposed method is one of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using our decryption method and key image, thus gets the original message.

B. Image Stenography

Steganography is the art and science of invisible communication. This is the hiding information in other information, thus hiding the existence of the communicated information. Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images [4], [5].Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information.

To ensure the security of the important message in communication, by the data hiding with image

Manuscript received January 6, 2014; revised August 1, 2014.

doi: 10.12720/lnit.2.2.172-176

cryptography. We proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image.

II. Related Work

Existing cryptographic and steganographic mediums suffer from a myriad of attacks. Johnson (1998) has studied such attacks on image steganography while Pal *et al*. (2002) has studied similar attacks in the context of audio steganography. Even though cryptography and steganography are exposed to so many probable attacks, very few people have given a thought to find alternate ways to transmit information. Fisk *et al*. (2002), point out the weaknesses of TCP/IP protocol suite and discuss how those weaknesses could be used as covert channels for secret communication, whereas Bao *et al*. (2002) focus on using communication accessories like email headers etc for secret communication.

A. Visual Cryptography

Visual Cryptography is a secret sharing scheme which uses the human visual system to perform computations. It received positive attention by the research community subsequent to its presentation by Naor and Shamir (1995) in the mid 90s. The basic principle behind visual cryptography is the use of superimposed images to reveal the secret. Each individual image can be considered as a cipher, and the corresponding image may be regarded as a key. It can also be interpreted as a graphical form of one time pad. Xiao *et al*. (2000) present a novel way to hide information with the aid of visual cryptography. They concealed a secret message using two innocent looking images [9], [10]. Once the two images were superimposed the secret text was revealed. They used a hybrid technique, which is a combination of visual cryptography and steganography to hide information. But Xiao *et al*. (2000) did not offer a disguising component to conceal the use of cryptography.

B. Image Cryptography

Image cryptography hasn't been widely studied as normal cryptography or visual cryptography. It was used by Zenon *et al*. (1997), to encode digital media (images and video) to provide confidentiality and intellectual property protection against unauthorized access. They proposed a version of digital image cryptography by using random phase mask for encrypting image. Here the authors consider image encoding as a new form of image encryption [11], [12]. They accomplish this using a transformation technique based on random phase masks. Their technique of encryption consists of four major steps [13]. Fourier transform of initial image, phase modification, inverse Fourier transform and finally image conversion. Zenon *et al*. (1997) used image cryptography and steganography to increase security, but they have not considered the use of image cryptography to disguise text cryptography, which would provide enhanced privacy and confidentiality in cryptographic communication.

C. Image Steganography

Image steganography has been widely studied by researchers. There are a variety of methodsusedin whichinformationcanbehiddeninimages. Some of them are described here [6]-[8].

- *Replacing least significant bit:* In image steganography almost all data hiding techniques try to alter insignificant information in the cover image. For instance, a simple scheme proposed by Chen, is to place the embedding data at the least significant bit(LSB)of each pixel in the cover image [Lee *et al*. 2000]. The altered image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc.
- *Replacing moderate significant bit:* Chan and Chang showed how to use the moderate significant bits of each pixel in the cover image to embed the secret message. This method improves sensitivity to modification, but it degrades the quality of stego-image.
- *Transformation domain techniques:* Other familiar data hiding techniques use the transformation domain of digital media to hide information [Chang *et al*. 2002, and Hsu *et al*. 1999]. Functions suchas the Discrete Cosine transform (DCT) and the discrete wavelet transform (DWT) are widely applied [Fabien *et al*. 1999, Chang *et al*. 2002, and Hsu *et al*. 1999]. These methods hide the messages in the significant areas of the cover image which makes them robust against compression, cropping and other image processing attacks.

III. Methodology

A. Read Image and Text

First, user given a secret message and choice a covered image.

```
>>user_entry = input('Enter a String?:', 's');
```

The response to the input prompt can be any MATLAB expression, which is evaluated using the variables in the current workspace.

user_entry = input('prompt') displays prompt as a prompt on the screen, waits for input from the keyboard, and returns the value entered in user_entry.

user_entry = input('prompt', 's') returns the entered string as a text variable rather than as a variable name or numerical value.

```
>> A = imread('circuit.tif');
```

A = imread(filename, fmt) reads a grayscale or color image from the file specified by the string filename. If the file is not in the current directory, or in a directory on the MATLAB path, specify the full pathname.

The text string fmt specifies the format of the file by its standard file extension.

Encryption process

ASCII Convert:
a=double(r);

B. Fibonacci Generate

In mathematics, the Fibonacci numbers or Fibonacci series or Fibonacci sequence are the numbers in the following integer sequence
0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

By definition, the first two numbers in the Fibonacci sequence are 0 and 1, and each subsequent number is the sum of the previous two.

In mathematical terms, the sequence Fn of Fibonacci numbers is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2} \tag{1}$$

With seed values

$$F_0 = 0, \quad F_1 = 1 \tag{2}$$

C. Random Number Matrix

out = randint(n,n,[1,100]);
out = randint generates a random scalar that is either 0 or 1,
with equal probability.
out = randint(m) generates an m-by-m binary matrix, each of whose entries independently takes the value 0 with probability 1/2.
out = randint(m,n) generates an m-by-n binary matrix, eachof whose entries independently takes the value 0 with probability 1/2.
out = randint(m,n,rg) generates an m-by-n integer matrix. Ifrg is zero, out is a zero matrix. Otherwise, the entries areuniformly distributed and independently chosen from the range

- [0, rg-1] if rg is a positive integer
- [rg+1, 0] if rg is a negative integer
- Between min and max, inclusive, if rg = [min,max] or[max,min]

D. Key and Encrypted Image

Key:
y = imcrop(x,[0 0 n n]);
Retrieving the coordinates of the crop rectangle.
imcrop copies a four-element position vector ([xminyminwidth height]) to the clipboard.
imwrite(y,'d:\b.tif');
imwrite(A,filename,fmt) writes the image A to the filespecified by filename in the format specified by fmt.
Encrypted image:
imwrite(r1,'d:\a.tif');
imwrite(A,filename,fmt) writes the image A to the file specified by filename in the format specified by fmt.
Read Key and Encrypted image
x2 = double(imread('d:\a.tif'));
x1 = double(imread('d:\b.tif'));
double(x) returns the double-precision value for X. If X isalready a double-precision array, double has no effect.
imread(filename, fmt) reads a grayscale or color imagefrom the file specified by the string filename. If the file isnot in the current directory, or in a directory on theMATLAB path, specify the full pathname.

E. Decryption Process

Result = Encrypted image – Key image
Read the Diagonal value of Result
Retrieve the left to right diagonal values of Z matrix
If i == j
M(i) = Z(i,j)

F. Fibonacci Generate

In mathematics, the Fibonacci numbers or Fibonacci seriesor Fibonacci sequence are the numbers in the following integer sequence
0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

By definition, the first two numbers in the Fibonaccisequence are 0 and 1, and each subsequent number is thesum of the previous two.

In mathematical terms, the sequence Fn of Fibonaccinumbers is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2} \tag{3}$$

With seed values

$$F_0 = 0, \quad F_1 = 1 \tag{4}$$

A. Convert ASCII to string:

char(X);
char(X) can be used to convert an array that containspositive integers representing numeric codes into aMATLAB character array.

IV. Flow of Work

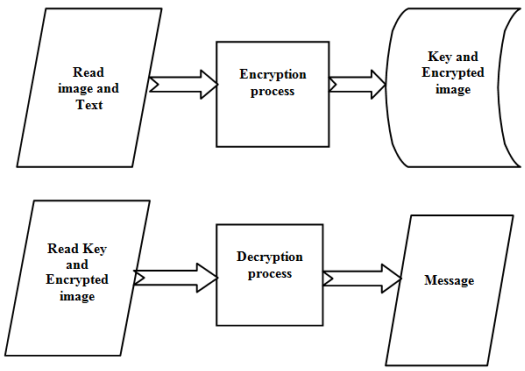

Figure 1: Diagram of flow of work

I am an Indian.

73	32	97	109	32	97	110	32	73	110	100	105	97	110	46

Length = 15

0	1	1	2	3	5	8	13	21	34	55	89	144	233	377

Sum=

73	33	98	111	35	102	118	45	94	144	155	194	241	343	423

Random Number 15 X 15 Matrix

82	15	71	49	76	35	8	61	11	14	42	14	55	31	21
91	43	4	45	26	20	6	27	97	87	5	95	30	51	31
13	92	28	65	51	26	54	66	1	58	91	96	75	52	48
92	80	5	71	70	62	78	69	78	55	95	58	19	82	24
64	96	10	76	90	48	94	75	82	15	50	6	69	80	85
0	66	83	28	96	36	13	46	87	86	49	24	19	65	20
28	4	70	68	55	84	57	9	9	63	34	36	37	38	23
55	85	32	66	14	59	47	23	40	36	91	83	63	82	18
96	94	96	17	15	55	2	92	26	52	37	2	79	54	23
97	68	4	12	26	92	34	16	81	41	12	5	9	36	44
16	76	44	50	85	29	17	83	44	8	79	17	93	94	32
98	75	39	96	26	76	80	54	92	24	39	65	78	88	93
96	40	77	35	82	76	32	100	19	13	25	74	49	56	44
49	66	80	59	25	39	53	8	27	19	41	65	44	63	19
81	18	19	23	93	57	17	45	15	24	10	46	45	59	91

Encoded message in the matrix:

73	15	71	49	76	35	8	61	11	14	42	14	55	31	21
91	33	4	45	26	20	6	27	97	87	5	95	30	51	31
13	92	98	65	51	26	54	66	1	58	91	96	75	52	48
92	80	5	111	70	62	78	69	78	55	95	58	19	82	24
64	96	10	76	35	48	94	75	82	15	50	6	69	80	85
0	66	83	28	96	102	13	46	87	86	49	24	19	65	20
28	4	70	68	55	84	118	9	9	63	34	36	37	38	23
55	85	32	66	14	59	47	45	40	36	91	83	63	82	18
96	94	96	17	15	55	2	92	94	52	37	2	79	54	23
97	68	4	12	26	92	34	16	81	144	12	5	9	36	44
16	76	44	50	85	29	17	83	44	8	155	17	93	94	32
98	75	39	96	26	76	80	54	92	24	39	194	78	88	93
96	40	77	35	82	76	32	100	19	13	25	74	241	56	44
49	66	80	59	25	39	53	8	27	19	41	65	44	343	19
81	18	19	23	93	57	17	45	15	24	10	46	45	59	423

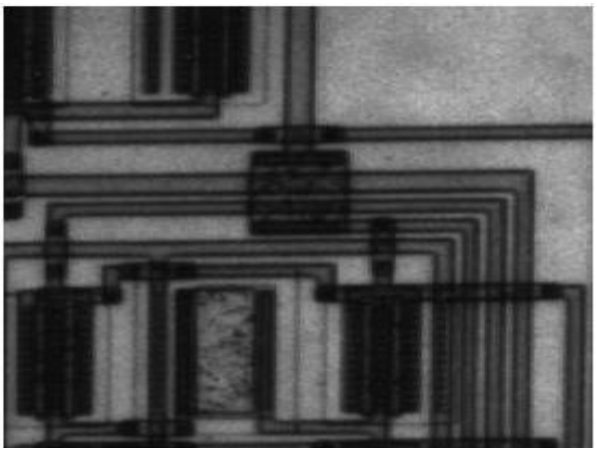

Figure 2. Crop image matrix

15	15	15	14	15	15	16	16	18	20	25	28	25	21	19
16	14	14	14	15	15	15	15	16	20	24	27	24	21	20
16	16	14	14	15	15	15	15	15	19	21	26	24	21	19
18	15	15	15	15	15	16	15	16	20	22	27	26	22	20
16	15	14	15	15	16	18	16	18	19	22	28	26	21	19
16	15	14	14	14	15	16	16	16	19	21	27	25	20	20
16	14	13	14	15	14	15	14	15	18	21	26	22	19	19
16	14	12	13	15	15	15	16	16	19	20	25	22	19	19
16	14	14	15	15	16	18	19	18	20	22	27	24	20	19
16	14	14	14	16	16	16	16	18	20	24	32	28	24	19
16	15	15	15	16	16	15	15	16	19	21	28	27	24	21
16	13	12	13	15	15	15	15	15	20	24	28	26	22	19
15	12	12	12	13	13	14	14	15	21	25	31	28	24	18
15	13	12	13	14	14	14	15	16	22	27	31	28	24	19
15	13	14	14	14	16	15	16	18	22	27	34	31	25	19

Encrypted matrix:

88	30	86	63	91	50	24	77	29	34	67	42	80	52	40
107	47	18	59	41	35	21	42	113	107	29	122	54	72	51
29	108	112	79	66	41	69	81	16	77	112	122	99	73	67
110	95	20	126	85	77	94	84	94	75	117	85	45	104	44
80	111	24	91	50	64	112	91	100	34	72	34	95	101	104
26	81	97	42	110	117	29	62	103	105	70	51	44	85	40
44	18	83	82	70	98	133	23	24	81	55	62	59	57	42
71	99	44	79	29	74	62	61	56	55	111	108	85	101	37
112	108	110	32	30	71	20	111	112	72	59	29	103	74	42
113	82	18	26	42	108	50	32	99	164	36	37	37	60	63
32	91	59	65	101	45	32	98	60	27	176	45	120	118	53
114	88	51	109	41	91	95	69	107	44	63	222	104	110	112
111	52	89	47	95	89	46	114	34	34	50	105	269	80	62
64	79	92	72	39	53	67	23	43	41	68	96	72	367	38
96	31	33	37	107	73	32	61	33	46	37	80	76	84	442

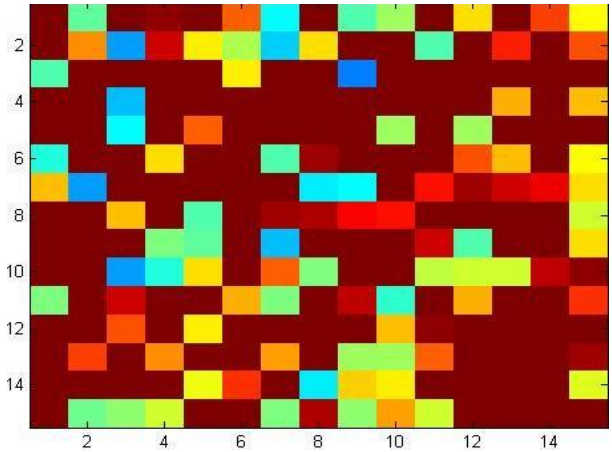

Figure 3. Encrypted image

Encrypted matrix

88	30	86	63	91	50	24	77	29	34	67	42	80	52	40
107	47	18	59	41	35	21	42	113	107	29	122	54	72	51
29	108	112	79	66	41	69	81	16	77	112	122	99	73	67
110	95	20	126	85	77	94	84	94	75	117	85	45	104	44
80	111	24	91	50	64	112	91	100	34	72	34	95	101	104
26	81	97	42	110	117	29	62	103	105	70	51	44	85	40
44	18	83	82	70	98	133	23	24	81	55	62	59	57	42
71	99	44	79	29	74	62	61	56	55	111	108	85	101	37
112	108	110	32	30	71	20	111	112	72	59	29	103	74	42
113	82	18	26	42	108	50	32	99	164	36	37	37	60	63
32	91	59	65	101	45	32	98	60	27	176	45	120	118	53
114	88	51	109	41	91	95	69	107	44	63	222	104	110	112
111	52	89	47	95	89	46	114	34	34	50	105	269	80	62
64	79	92	72	39	53	67	23	43	41	68	96	72	367	38
96	31	33	37	107	73	32	61	33	46	37	80	76	84	442

+

Key matrix

15	15	15	14	15	15	16	16	18	20	25	28	25	21	19
16	14	14	14	15	15	15	15	16	20	24	27	24	21	20
16	16	14	14	15	15	15	15	15	19	21	26	24	21	19
18	15	15	15	15	15	16	15	16	20	22	27	26	22	20
16	15	14	15	15	16	18	16	18	19	22	28	26	21	19
16	15	14	14	14	15	16	16	16	19	21	27	25	20	20
16	14	13	14	15	14	15	14	15	18	21	26	22	19	19
16	14	12	13	15	15	15	16	16	19	20	25	22	19	19
16	14	14	15	15	16	18	19	18	20	22	27	24	20	19
16	14	14	14	16	16	16	16	18	20	24	32	28	24	19
16	15	15	15	16	16	15	15	16	19	21	28	27	24	21
16	13	12	13	15	15	15	15	15	20	24	28	26	22	19
15	12	12	12	13	13	14	14	15	21	25	31	28	24	18
15	13	12	13	14	14	14	15	16	22	27	31	28	24	19
15	13	14	14	14	16	15	16	18	22	27	34	31	25	19

=

73	15	71	49	76	35	8	61	11	14	42	14	55	31	21
91	33	4	45	26	20	6	27	97	87	5	95	30	51	31
13	92	98	65	51	26	54	66	1	58	91	96	75	52	48
92	80	5	111	70	62	78	69	78	55	95	58	19	82	24
64	96	10	76	35	48	94	75	82	15	50	6	69	80	85
0	66	83	28	96	102	13	46	87	86	49	24	19	65	20
28	4	70	68	55	84	118	9	9	63	34	36	37	38	23
55	85	32	66	14	59	47	45	40	36	91	83	63	82	18
96	94	96	17	15	55	2	92	94	52	37	2	79	54	23
97	68	4	12	26	92	34	16	81	144	12	5	9	36	44
16	76	44	50	85	29	17	83	44	8	155	17	93	94	32
98	75	39	96	26	76	80	54	92	24	39	194	78	88	93
96	40	77	35	82	76	32	100	19	13	25	74	241	56	44
49	66	80	59	25	39	53	8	27	19	41	65	44	343	19
81	18	19	23	93	57	17	45	15	24	10	46	45	59	423

73 33 98 111 35 102 118 45 94 144 155 194 241 343 423

0 1 1 2 3 5 8 13 21 34 55 89 144 233 377

73 32 97 109 32 97 110 32 73 110 100 105 97 110 46

I am an Indian.

V. Algorithm

A. Encryption

1. START
2. M → Read a text message from user.
3. C → Convert Message to ASCII code using double function in Matlab
4. N → Calculate the length of the message
5. F → Generate the Fibonacci series up to N
6. T→Transpose the F matrix
7. S → Addition of C and T matrix
8. R → Generate Random number 1 to 100 by randint( ) and store it N X N matrix
9. Generate a (N x N) matrix

   If i==j

   A(i,j) → S(i)

   Else

   A(i,j) →R(i,j)
10. X → Read a Image by imread function
11. Y → Crop the image by imcrop(X,[0 0 N N])
12. G → Change the data type of Y to double by double()
13. Write the matrix G as image format in the memory by imwrite()
14. E → Adding two Matrix of A and G
15. Write the matrix E as image format in the memory by imwrite()
16. STOP

B. Decryption

1. START
2. D → Read The Encrypted image from memory
3. B →Read the Key image from memory
4. Z → Subtraction of D and B matrix
5. N1 → Calculate the length of Z
6. M → Retrieve the left to right diagonal values of Z matrix

   If i==j

   M(i) → Z(i,j)
7. M1 → Transpose the M matrix
8. E → Generate the Fibonacci series up to N1
9. E1→Transpose the E matrix
10. P → Subtraction of M1 and E1
11. Result → Convert ASCII to String and show the message.
12. STOP

VI. Conclusion

In this paper we proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image.

References

[1] A. Sinkov, *Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America*, 1966.

[2] G. R. Blakely, "Safeguarding cryptographic keys," in *Proc. National Computer Conf.*, vol. 48, pp. 313–317.

[3] Z. G. Ma and S. S. Qiu, "An image cryptosystem based on general cat map," *J. China Inst. Commun.*, vol. 24, pp. 51-57, 2003.

[4] T. Kong and Z. Dan, "A new anti-arnold transform algorithm," *J. Software*, vol. 15, pp. 1558-1564, 2004.

[5] C. Y. Hong and W. G. Zou, "Digital image scrambling technology based on three dimensions arnoldtransform and its period," *J. Nanchang Univ. Nat. Sci.*, vol. 29, pp. 619-621, 2005,

[6] Z. H, "On the period of 2D Random matrix scrambling transform and its application in image hiding," *Chinese J. Comput.*, vol. 29, pp. 2218-2225, 2006.

[7] D. L. Yang, N. Cai, and G. Q. Ni, "Digital image scrambling technology based on the symmetry of arnold transform," *J. Beijing Inst. Technol.*, vol. 15, pp. 216-220, 2006.

[8] M. Mishra, A. R. Routray, and S. Kumar, "High security image steganography with modified Arnold's cat map," *IJCA*, vol. 37, no. 9, pp. 16-20, January 2012.

[9] M. Mishra, S. Kumar, and S. Mishra, "Security enhanced digital image steganography based on successive arnold transformation," *Advances in Intelligent and Soft Computing*, vol. 167, pp. 221-229, 2012.

[10] D. X. Qi, J. C. Zou, and X. Y. Han, "A new class of transform and its application in the image transform covering," *Sci. China (Series E)*, vol. 43, pp. 304-312, 2000.

[11] J. C. Zou, R. K. Ward, and D. X. Qi, "A new digital image scrambling method based on Fibonacci numbers," in *Proc. International Symposium on Circuits and Systems*, Vancouver, Canada, May 23-26, 2004, pp. 965-968,.

[12] J. C. Zou, R. K. Ward, and X. D. Qi, "The generalized fibonaci transformations and application to image scrambling," in *Proc. IEEE International Conference on Acoustic, Speech and Signal Processing*, Canada, May 17-21, 2004, pp. 385-388.

[13] L. P. Shao, Z. Qin, H. J. Gao, and X. C. Heng, "2D triangular mappings and their applications in scrambling rectangle image," *Information Technology Journal*, vol. 7, pp. 40-47, 2008.

Manoj Mukherjee Date of place – Bankura, Date of Birth – 9th May, 1993.He had received a BCA (Hons) degree from Burdwan Institute of Management and Computer Sceience, Burdwan, West Bengal under The University of Burdwan in the year 2013. He is currently studying MCA I semesterin AIT, Bangalore under VTU (Visvesvaraya Technological University, Belgaum). He is interest in the field of image processing and cryptography. He has Publish 2 international journal.

Prof. Debabrata Samanta, a member of the IAENG, Board member of the Seventh Sense Research Group Journals (SSRGJ). He obtained his B.Sc. (Physics Honors) in the year 2007, from the Vivekananda Collage, Takurpukur, under Calcutta University; Kolkata, India .He obtained his MCA in the year 2010, from the Academy Of Technology, under WBUT. He has been working his PhD in Computer Science and Engg. from the year 2010 from National Institute of Technology, Durgapur, India in the area of Image Processing .He ispresently working as a Assistant Professor of MCA dept in Acharya Institute of Technology, Bangalore, Karnataka, India from 19th Aug,2013. His areas of interest are Artificial Intelligence, Natural Language Processing and Image Processing. He has published 63 papers in International Journals / Conferences.