DUAL SECURITY

[1] Satish Patil, [2] Pravin Tangle, [3] Nidhi Poonia
[1] Student, [2] Student, [3] Assistant Professor
[1] MCA,
[1] BVIMIT, Navi Mumbai, India

Abstract : Dual security is combination of two Cryptography and Steganography techniques are used for secured communication between sender and receiver. Data or message security is one of main requirement in today's world, because of various attackers we combined these two techniques to provides higher level security as compare to existing technique. Cryptography convert message from readable format(plain text) to non-readable format(cipher text) and Steganography hides visibility of the message. By using RC6 algorithm Cryptography is done and the output of cryptography is taken as input to perform Steganography and gives final output. This paper presents combination of two techniques which provide higher security while communication is happening between users.

Keywords – Stegnography, Cryptography, Authentication, Integrity, Confidentiality, RC6.

I. Introduction

Dual Security is a Combination of Cryptography and Steganography is known as Dual Security.

1.1. Cryptography

Cryptography [1][2] means converting plain text into cipher text. Objectives of cryptography are converting information in non-readable format so that only intended recipient convert it in readable format. Process of making cipher text is known as Encryption. Process of getting same plain text from cipher text is known as Decryption.

1.2. Steganography

It is an art and science of hiding the visibility of message. Steganography hides the message so that only intended receiver knows that existence of message. Message can be hides within text, image, audio or video. The main advantage of Steganography [3] is that the normal user or hackers doesn't have idea of message actually exist.

II. Kind of Security

There are 3 kinds of security they are as follows

2.1. Authentication

Authentication is process in which user inputs are comparing to information which stored in database. If user inputs match with information stored in database it means user successfully authenticated else authentication failed. For example username and password.

2.2. Confidentiality

Confidentiality [4] is the protection of personal information. Confidentiality means keeping a client's data or information between you and the client. Sensitive data or information should be disclosed to authorize user only. Main objective of Confidentiality is data must be read and understood only by intended receiver or receivers. It can be achieved through encryption.

2.3. Integrity

Integrity [4] means maintaining and assuring the accuracy and consistency of data when it travels from one end to another. Data must not be changed during its transmission. Main objective of Integrity is to ensure data cannot be altered or modified by unauthorized user. It makes sure that nobody in between sender and receiver can change and shared data. It achieved by using cryptography algorithm.

III. Algorithm and Technique

There are many cryptographic techniques available among them AES is one of the most powerful technique.

3.1. RC6

RC6 derived from RC5 and it is symmetric key block cipher. It was developed by Ron Rivest, Matt Robshaw, Ray Sidney and Yiqun Lisa Yin. It is designed to meet requirements of Advanced Encryption Standard (AES) [5].It is an improvement of RC5.Like RC5, RC6 makes essential use of data-independent rotation. New features of RC6 include the use of four working register instead of two.RC6 .has block size of 128 bits and supports key size of 128,192 and 256 bits.RC6 provides greater security, fewer rounds and increased throughput.

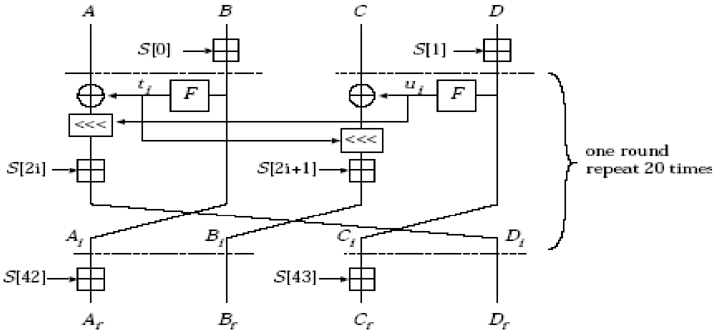


fig: 1

3.2. Key Features

1) Symmetric Block cipher.
2) RC6- w/r/b:
w= word size in bits.
r= no. of rounds.
b= key size in bytes.
3) Key length-266bytes (i.e. 2040 bits)
4) No. of trials required to break key=2^{2040}
5) Greater security.
6) High resist towards attack than previous algo.

3.3. Steps for Encryption and Decryption

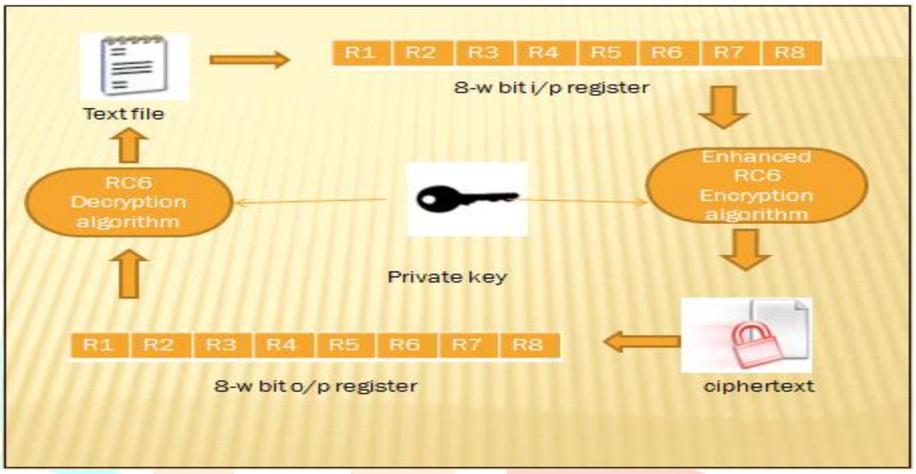


fig: 2

IV. STEGANOGRAPHY

4.1. Image steganography

It is an art and science of communicating in a way which hides the presence of communication. Steganography hides the message so it cannot be seen. It is a technology that embeds confidential message within text or digital picture or digital audios or digital videos. Here I'm using image Steganography. Which means data or information hidden in image? Which is extremely difficult to detect existence of message?

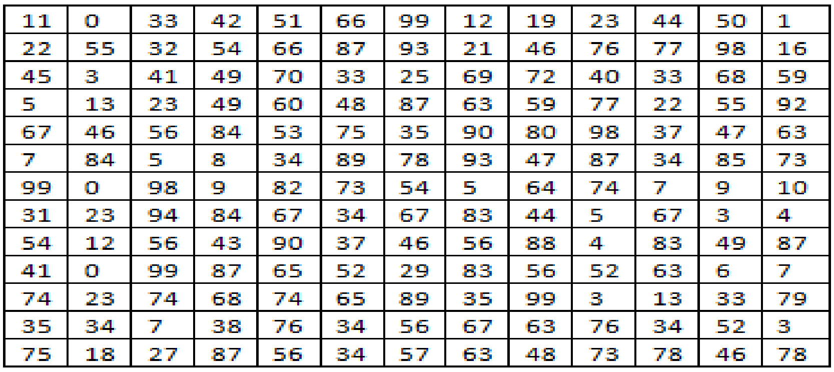
V. METHODOLOGY

5.1. Fibonacci series

Fibonacci [6] series start with 0 and 1, and each upcoming number is sum of two previous numbers.
It uses Seed values as F0=0, F1=1
In Mathematical terms:- Fn=Fn-1+Fn-2
0,1,1,2,3,5,8,13,21,34,55,89,144…..
Example-
Good Morning.
1 23 55 60 88 34 75 99 12 22 19 81 39
Length=13(Fibonacci series numbers)
0 1 1 2 3 5 8 13 21 34 55 89 144
Sum=
1 24 56 62 91 39 83 112 33 56 74 170 183

5.2. Random Number 13 * 13 Matrix

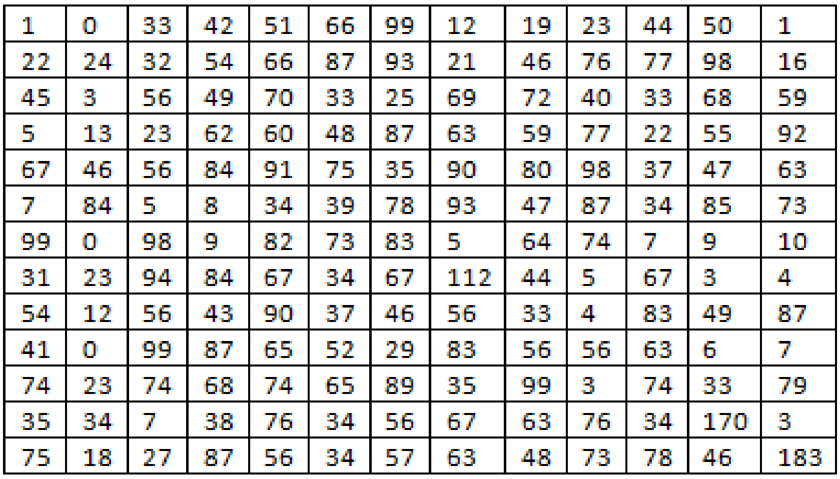
Table: 1



11	0	33	42	51	66	99	12	19	23	44	50	1
22	55	32	54	66	87	93	21	46	76	77	98	16
45	3	41	49	70	33	25	69	72	40	33	68	59
5	13	23	49	60	48	87	63	59	77	22	55	92
67	46	56	84	53	75	35	90	80	98	37	47	63
7	84	5	8	34	89	78	93	47	87	34	85	73
99	0	98	9	82	73	54	5	64	74	7	9	10
31	23	94	84	67	34	67	83	44	5	67	3	4
54	12	56	43	90	37	46	56	88	4	83	49	87
41	0	99	87	65	52	29	83	56	52	63	6	7
74	23	74	68	74	65	89	35	99	3	13	33	79
35	34	7	38	76	34	56	67	63	76	34	52	3
75	18	27	87	56	34	57	63	48	73	78	46	78

5.3. Encoded Message in the Matrix

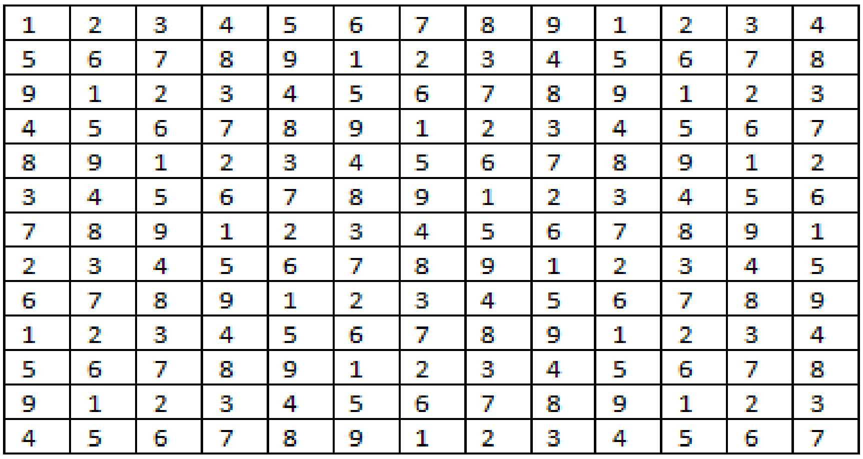
Table: 2



1	0	33	42	51	66	99	12	19	23	44	50	1
22	24	32	54	66	87	93	21	46	76	77	98	16
45	3	56	49	70	33	25	69	72	40	33	68	59
5	13	23	62	60	48	87	63	59	77	22	55	92
67	46	56	84	91	75	35	90	80	98	37	47	63
7	84	5	8	34	39	78	93	47	87	34	85	73
99	0	98	9	82	73	83	5	64	74	7	9	10
31	23	94	84	67	34	67	112	44	5	67	3	4
54	12	56	43	90	37	46	56	33	4	83	49	87
41	0	99	87	65	52	29	83	56	56	63	6	7
74	23	74	68	74	65	89	35	99	3	74	33	79
35	34	7	38	76	34	56	67	63	76	34	170	3
75	18	27	87	56	34	57	63	48	73	78	46	183

5.4. Crop image Matrix

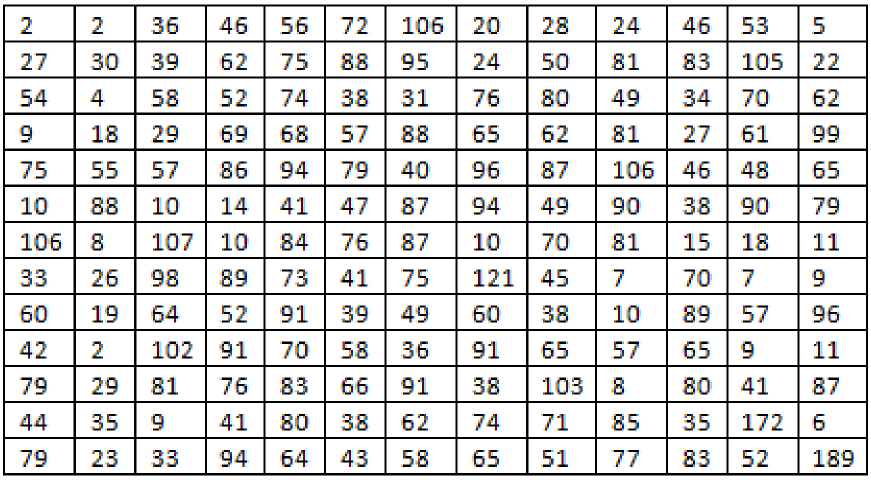
Table: 3



1	2	3	4	5	6	7	8	9	1	2	3	4
5	6	7	8	9	1	2	3	4	5	6	7	8
9	1	2	3	4	5	6	7	8	9	1	2	3
4	5	6	7	8	9	1	2	3	4	5	6	7
8	9	1	2	3	4	5	6	7	8	9	1	2
3	4	5	6	7	8	9	1	2	3	4	5	6
7	8	9	1	2	3	4	5	6	7	8	9	1
2	3	4	5	6	7	8	9	1	2	3	4	5
6	7	8	9	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	1	2	3	4
5	6	7	8	9	1	2	3	4	5	6	7	8
9	1	2	3	4	5	6	7	8	9	1	2	3
4	5	6	7	8	9	1	2	3	4	5	6	7

5.5. Encrypted Matrix

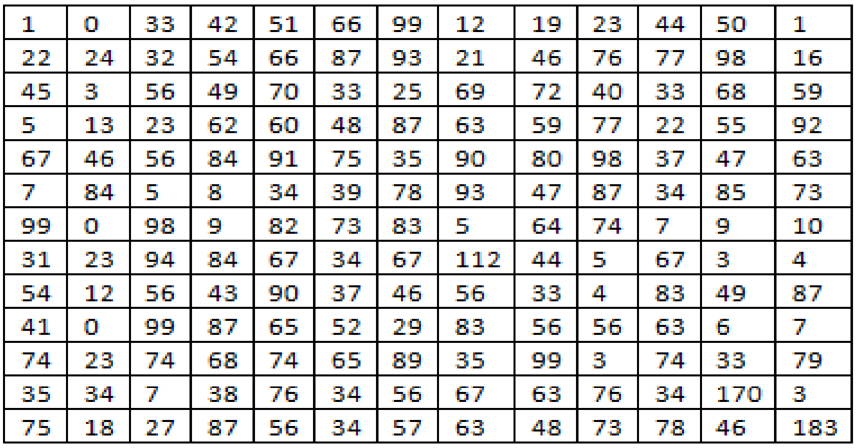
Table: 4



2	2	36	46	56	72	106	20	28	24	46	53	5
27	30	39	62	75	88	95	24	50	81	83	105	22
54	4	58	52	74	38	31	76	80	49	34	70	62
9	18	29	69	68	57	88	65	62	81	27	61	99
75	55	57	86	94	79	40	96	87	106	46	48	65
10	88	10	14	41	47	87	94	49	90	38	90	79
106	8	107	10	84	76	87	10	70	81	15	18	11
33	26	98	89	73	41	75	121	45	7	70	7	9
60	19	64	52	91	39	49	60	38	10	89	57	96
42	2	102	91	70	58	36	91	65	57	65	9	11
79	29	81	76	83	66	91	38	103	8	80	41	87
44	35	9	41	80	38	62	74	71	85	35	172	6
79	23	33	94	64	43	58	65	51	77	83	52	189

5.6. Decrypted Matrix= Encrypted Matrix - Crop image Matrix (key matrix)

Table: 5



1	0	33	42	51	66	99	12	19	23	44	50	1
22	24	32	54	66	87	93	21	46	76	77	98	16
45	3	56	49	70	33	25	69	72	40	33	68	59
5	13	23	62	60	48	87	63	59	77	22	55	92
67	46	56	84	91	75	35	90	80	98	37	47	63
7	84	5	8	34	39	78	93	47	87	34	85	73
99	0	98	9	82	73	83	5	64	74	7	9	10
31	23	94	84	67	34	67	112	44	5	67	3	4
54	12	56	43	90	37	46	56	33	4	83	49	87
41	0	99	87	65	52	29	83	56	56	63	6	7
74	23	74	68	74	65	89	35	99	3	74	33	79
35	34	7	38	76	34	56	67	63	76	34	170	3
75	18	27	87	56	34	57	63	48	73	78	46	183

```
1  24  56  62  91  39  83  112  33  56  74  170  183
 -
0  01  01  02  03  05  08  013  21  34  55  089  144

Ans =
1  23  55  60  88  34  75  099  12  22  19  081  039
Good Morning.
```

5.7. Steps

1) Count number of characters in message (include space and dot (.)) and take same length of random numbers.
2) Take same length of Fibonacci series numbers as message length (13).
3) Perform addition of numbers presents in step1 and step2.
4) Take 13*13 random number matrix.
5) Encode output of step3 in 13*13 random number matrix in particular pattern (i.e horizontal, vertical).
6) Take any image and divide image in 13*13 matrix.
7) Perform addition of step5 and step6 matrix and get final output. Send it to the intended receiver.
8) Receiver performs reverse steps to get original message which comes from sender side.

VI. Conclusion

This paper has presented the results of a study on cryptography and steganography techniques which are used for secured communication between sender and receiver for future security. We combined these two techniques to provide higher level security as compare to existing technique.

The combined compression of steganography and cryptography is a forceful tool which empowers people to communicate without possible bug uniform knowing there is a form of communication in the first place.

References

[1] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134

[2] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210

[3] Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY & PRIVACY

[4] https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/

[5]J. Nechvatal, et. al., Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000, available at [1].

[6] Fibonacci and Lucas numbers, and the Golden Section: Theory and Applications, S Vajda, Dover Press(2008).