An Alphanumeric Symmetric Key Cryptography Algorithm for Fast and Secure Enciphering

Suraj Verma
Dept. of Computer Science
SRMSCETR (Bareilly), India

Ashish Agrawal
Dept. of Computer Science
SRMSCETR (Bareilly), India

ABSTRACT

Since the time of human development there has been a need to shield delicate data from falling into wrong hands. To accomplish this security human has depended on a branch of science known as morse alphabet. A few subsections of morse alphabet are accessible like, Multivariate morse alphabet, Quantum morse alphabet, DNA morse alphabet, Symmetric key morse alphabet, Visual morse alphabet, Steganography, and so on. This paper propose a quick, secure and straightforward enciphering conspire .The technique is appropriate for substantial record and additionally littler .In this paper the execution is contrast and the mainstream enciphering calculations and the outcome demonstrate that the suggested plan is all the more secure then other conventional enciphering plans. The suggested calculation is straightforward modular addition based calculation.

Keywords

Symmetric key morse alphabet, Unencrypted concontext, cipher concontext s.v calculation.

1. INTRODUCTION

Security is the most important Concern in the communication and morse alphabet carry an important part of it .Most of the security algorithms and thet are using now days only focus on security. But performance is also very important and our main concern is to get batter algorithm.Nothing is secure over the internet and the way and thet is using for the communication is depends upon internet. Secure data transmission is an challenging field.We use mainly two categoryof key based methods one is a symmetric key morse alphabet and another is asymmetric key morse alphabet.In symmetric key morse alphabet, both enciphering and deciphering are performed with the same key. While in public key morse alphabet use two different keys, one for enciphering and one for deciphering. [30]

In the suggested algorithm both have same size cipher concontext and the unencrypted concontext. The ASCII estimation of the every last in the unencrypted concontext will be subtracted from the relating ASCII estimation of the key .

At that point the relating character will be composed as the estimation of that letter in figure report. The qualities are taken at run time and in addition the determination of the key is additionally given to the clients wish if the principal event of the letter "x" relates to the "@"or "5" or anything in light of the position of the record pointer in the report. So "x" can have a greatest of 256 likely values, including a similar esteem. later on we utilize the expression "S.V Calculation" rather than suggested calculation S.V remain for Suraj Verma including a similar esteem. later on utilize the expression "S.V Calculation" rather than suggested calculation S.V remain for Suraj Verma. Whatever remains of the segment is talked about as takes after: Segment 2 keeps up the rundown of different morse alphabet systems in practices. Section3, outline detail of the suggested approach is talked about. The security issue and different assaults that the framework may face is appeared in segment 4. Lastly the segment 5. incorporates the finish of the suggested framework.

2. BACKGROUND

Secure information transmission is the fundamental need of all parts. Due to these morse alphabet, having this much significance in this present reality. There is a wide assortment of morse alphabet technique and in addition a few enciphering plans like Multivariate morse alphabet, Quantum morse alphabet, DNA morse alphabet, Symmetric key morse alphabet, Steganography, Visual morse alphabet and so forth.With such a large count of various elements

Symmetric key morse alphabet mostly classified into stream cipher and block cipher. The greater part of the square figures rely on upon the fiestel organize and certain annular. This count of annular make it tedious than stream figures [5], [30]. Stream figures are quick and in addition straightforward. Equipment unpredictability of a stream figure is additionally less. It is utilized as a part of utilizations where a lot of information should be considered with to a great degree high throughput and low unpredictability equipment [30].

In One Time pad (OTP) a code is used generated randomly.This is done with the help of code booklet. Random count collection are present in every OTP. This opt used exactly once and the size of the key is fixed. And after using this OTP it will discarded this is one of the most secure approaches.

Vernam figure, a symmetric stream figure and thet joins unencrypted content with an irregular or pseudorandom key to frame the Figure content. The key and the unencrypted content are of a similar length.The distinction amongst OTP and the vernam figure is that OTP has genuine arbitrariness though vernam figure will rehash after a time of times. RC4 is a sort of vernam figure .

A well-known cryptographic calculation is a booklet figure in and thet it takes a booklet or a piece of it as a symmetric key. They scramble the Unencrypted content by supplanting the word in the Unencrypted content with the position of that word in the booklet. On the off chance that we utilize the "Ramayana" it is known as 'Ramayana Figure'. The burden of this approach is the point at and thet the booklet doesn't have the word and thet we expected to scramble. So there is no conceivable word in booklet to supplant with unencrypted content. The issue can deal with up to a specific level by the utilization of the word reference. But in the suggested system, it is possible to use the new key at every time like OTP or previously used key like vernam cipher. It is absolutely depends upon a user’s wish. So this is the combination of both.

3. DESIGN DETAILS

Morse alphabet is an enormous range and each association has some secret data or information and thet must be protected or remained careful. Hence numerous cryptographic plans are utilized. Regular morse alphabet is one of them, in and thet we utilize complex operations like moving, change, transposition, extending and change. This suggested approach presents another cryptographic technique and thet is straightforward however difficult to break. The suggested calculation is changed adaptation of OTP. The suggested technique delivers similarly estimated figure content. Length of the unencrypted content record fortifies the figure content. as the span of the unencrypted content record increment figure content turns out to be all the more effective. In OTP, the OTP is utilized once and afterward discarded.In OTP producing the key while in the S V calculation, it relies on client to choose the key.Because of the key determination is arbitrary, the measure of conceivable change increment tremendously.For each character "k" might be 256 conceivable changes. Similarly, every character in the document is having such 256 conceivable changes. The quantity of conceivable changes rely on upon the length of the unencrypted content. S.V Calculation changes over a cipherconcontext of a similar size. S-V Calculation can have a greatest conceivable change and thet is a 256 power count of characters in the unencrypted content.

(s) n … .. (1)

Where,

S: - Count of changes conceivable

N: - Count of characters in unencrypted content A.

3.1 Enciphering

Input the unencrypted content to be encoded and the key. The key can be a document of any size as indicated by the client's desire. That is, the key record is chosen by the client. Hence the multifaceted nature level is additionally picked by the client. This fluctuates for every last time in light of the fact that the key document is chosen arbitrarily by the client. So that the cryptanalysts not able to discover any likenesses with any two diverse figure writings. It takes the main character of the unencrypted content record and the primary character of the key document and plays out a subtraction operation and thet is the principal character of the figure content et cetera

The operation is given by :

1. Encrypt the key by using step 4.
2. Reverse the plaintext by using step 5
3. (message + key) mod(256)

The thesis work (proposed algorithm) is executed in matlab. They are quick and strong. The algorithm is given underneath:

3.1.1 Steps for the Plain Text Encryption

Step 1: Perused the plain text. locate the comparing ASCII value of every letter of message (n1).

Step 2: Take the key chosen by the client and locate the relating ASCII estimation of each letter of (y).
Step 3: count the length of the key(y).and generating some of the integers value.
Step 4: Add the integer value of the key with every letter of the key ,with these following steps.

```
while(y~=0)
        key2(x)=key2(x)+rem(y,10);
        y=idivide(y,10);
```

step 5 :reverse the plain text by

```
      mes=me;
       for x=1:k
           me(x)=mes(k+1-x);
```

Step 6: compare the length of n1 with the length of y and follows these steps.

Step 6.1 If (n1>key2(x))
{
Step 6.2: Move KEY file pointer to point starting.

Step 6.3: Move plain text file position backward from current file position by n1-n2 times }
Step 6.4: endif.
Step 7: Add the ASCII value of plain text(n1) to the ASCII value of key(y).with mod of 256.
Step 8: Print the cipher text.

Lets take a simple example to implement the algorithm.

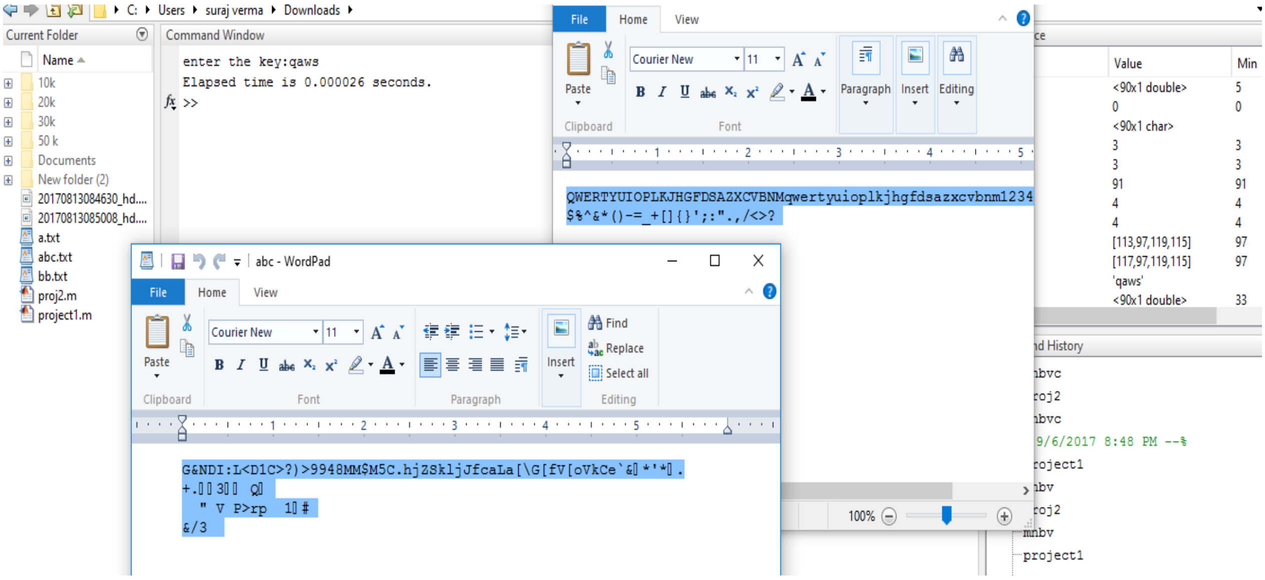
Plaintext cryptography
Riverse plaintext yhpargotpyrc
Key m*?7

RP	key	p+k mod(256)	ciphertext
y = 121	**m =109**	**230**	**æ**
h = 104	***=42**	**146**	**’**
p = 112	**? =63**	**175**	**¯**
a = 97	**7=55**	**152**	**˜**
r = 114	**m=109**	**223**	**ß**
g = 103	***=42**	**145**	**‘**
o = 111	**?=63**	**174**	**®**
t = 116	**7=55**	**171**	**«**
p = 112	**m=109**	**221**	**Ý**
y = 121	***=42**	**163**	**£**
r = 114	**?=63**	**177**	**±**
c =99	**7=55**	**154**	**š**

Fig 1. Encryption

Plain text is **cryptography**
And the key is **m*?7**
Ciphertext is **æ’ ¯˜ ß ‘®« Ý£ ± š .**

The programming dialect and thet we used to process this approach is MATLAB for enciphering. On account of enciphering, three contentions are acknowledged into the program. The initial one is the unencrypted content record. The second one is the KEY document. The third one is the yield document to store the final figure content. Then again, while decoding the figure Content utilize three contentions itself. The main contrast is that the primary contention is the figure message rather than the unencrypted content record.
The KEY document might be not exactly or equivalent to the unencrypted content, subtract ASCII estimation of each letter of unencrypted content from the ASCII benefit of comparing letter in the key record. Compose the subtracted values into the figure content. On the off chance that the count key document letters are littler than the unencrypted content letters, on the other hand, begin with the primary letter of the key record for subtracting the rest of the estimation of the unencrypted content Then the circle is executed until the finish of unencrypted content document is found. Consider the accompanying illustration:



```
enter the key:qaws
Elapsed time is 0.000026 seconds.
>>
```

```
QWERTYUIOPLKJHGFDSAZXCVBNMqwertyuioplkjhgfdsazxcvbnm1234
$%^&*()-=_+[]{}';:".,/<>?
```

```
G&NDI:L<D1C>?)>9948MM$M5C.hjZSkljJfcaLa[\G[fV[oVkCe`&▯*'*▯.
+.▯▯3▯▯ Q▯
 " V P>rp  1▯#
&/3
```

```
Value              Min
<90x1 double>      5
0                  0
<90x1 char>
3                  3
3                  3
91                 91
4                  4
4                  4
[113,97,119,115]   97
[117,97,119,115]   97
'qaws'
<90x1 double>      33
```

Fig 2. Encryption Implementation

Plaintext
QWERTYUIOPLKJHGFDSAZXCVBNMqwertyuioplkjhgfdsazxcvbnm1234567890!@#$%^&*()-=_+[]{}';:".,/<>?

Key **qaws**

Ciphertext
G&NDI:L<D1C>?)>9948MM$M5C.hjZSkljJfcaLa[\G[fV[oVkCe`&_*'*_.+.__3___Q_
__"_V_P>rp__1_#
&/3

In this case the unencrypted concontext is "". By using key as "QWERTYUIOPLKJHGFDSAZXCVBNMqwertyuioplkjhgfdsazxcvbnm1234567890!@#$%^&*()-=_+[]{}';:".,/<>?" .

In fig.1 the framework delivers the figure content. And the unscrambling side although the key "**qaws**" is connected the subsequent unscrambled message will be "QWERTYUIOPLKJHGFDSAZXCVBNMqwertyuioplkjhgfdsazxcvbnm1234567890!@#$%^&*()-=_+[]{}';:".,/<>?". Here the key record is chosen by the client itself. At whatever point the saltine exploits to split the figure content may come about some important message and the wafer will be muddled. Another imperative comment is that the key document require not to have an indistinguishable length from that of plain concontext record, it can have littler, bigger or even equivalent to the plain concontext record length. This makes the enciphering conspire more vigorous and truly nonbreakable.

4. PERFORMANCE ANALYSIS

The performance analysis can be done with various measures such as

1) File size (in KB) Vs Execution Time (in ms)
2) Comparison between different algorithms1
3) Message size (in KB) Vs Throughput (in MBPS)
4) Cipher Text Length (in Bytes) Vs Years to Crack

Table . 1 Comparision between Different Algotithms for Decryption Time for Different Key Size

Name of algorithm	Key size Bit	Number of alternative key	Time requirwd at one decryption /micro Second	Time required at 10^6 decryption/mocro econds
BLOW FISH	32	4.3*10^9	35.8 minuts	2.15 millisec onds
DES,RC4	56	7.2*10^16	1142 years	10.01 hours
AES	128	3.4*10^38	5.4*10^24 years	5.4*10^18 years
AES	168	3.7*10^50	5.9*10^36 years	5.9*10^30 years
POLYALPHABATIC	26Char(parmutetion)	4*10^26	6.4*10^12	6.4*10^6 years
A S ALGO	256 character	(256)^n n=1,2,3,5,…. …. If n=20.	4.6*10^31 years	4.6*10^28 years

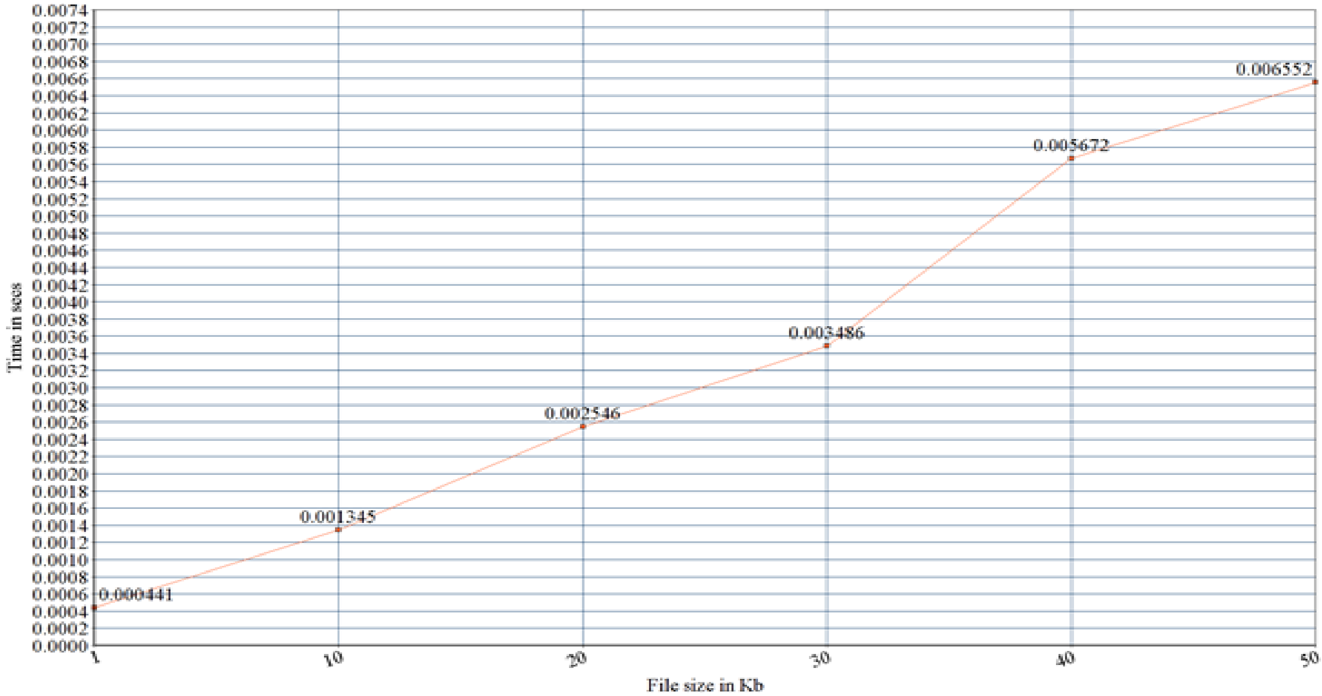


Fig .3 Encryption Time(sec) for Different Key Size

Table . 2 Encryption Decryption for different Plain Text Size (KB)

File Size In KB	Encryption Time In Second	Encryption Decryption Time In Second
1	0.000441	0.00019
10	0.001345	0.001892
20	0.002546	0.002241
30	0.003486	0.003247
40	0.005672	0.005016
50	0.006552	0.005859

5. ATTACKS AND SECURITY ISSUES

5.1 Commonplace Assaults

There are a few sorts of assaults present in the system. These incorporate the savage constrain assault, time/memory/information tradeoff assault, partition and overcome assault and recognizing assault.

5.2. Savage constrain assault

The beast drive assault can be stayed away from in this proposed paper (proposed algorithm). Since animal constrain assault is working in light of attempting every single probability. Here the quantity of most extreme potential outcomes is given by:

(s) n. … . (4)

Where,

S :- Count of changes conceivable

N :- Count of characters in unencrypted content

In this way, the likelihood to break the unencrypted content is given by :

1/(s)n … (5)

1/(256)1 ,1/(256)2, 1/(256)3, … … (6)

5.3 Time/memory/information Tradeoff

Time/memory/information tradeoff assault can likewise be kept away from since there is no settled key and thet is having any likeness. Since this assault works in light of a precomputed table. Here the key document is chosen by the client itself and additionally he utilizes it just once. Along these lines, it can not have a settled change table. So that Time/memory/information tradeoff assault can be killed.

5.4. Separate and Overcome Assault

Gap and vanquish assault or relationship assault goes under known unencrypted content assault. That is, the unencrypted content and additionally the figure content will be accessible for the aggressor. This assault chips away at the suspicion that the key stream will be produced by joining the yield of a few LFSRs (direct input shift registers). A-S Calculation does not utilizes any LFSRs. It is not having any settled change or key era calculation so that the key won't have any similitudes. The key document is chosen by the client at run time. So that there are no predefined changes accessible and thet will help in cracking the figure. Along these lines the likelihood of separation and vanquish assault can without much of a stretch be counteracted. Since we can't foresee and thet kind of record he is utilizing.

5.5 Recognizing Assault

A recognizing assault is a sort of assault that enables an assailant to make sense of the encoded information from the irregular information. It implies that if there exists a connection between various figure writings or between unencrypted content and figure message the aggressor can make utilization of it. A-S Calculation has been much the same as a one-time cushion and thet can have a client chose key record of obscure sort (as chosen by the client)

6. CONCLUSION

In this paper ("An Alphanumeric Symmetric Key Morse alphabet Algorithm for Fast and Secure Enciphering"), have suggested an exceedingly effective and nonbreakable enciphering conspire for secure information transmission. The likelihood to break the unencrypted content abatements in light of the fact that, there is no change table or precomputed table is available. Giving the capacity to clients to choose the key record without anyone else's input makes this proposed algorithm into an alternate level. The examination of the suggested framework demonstrates that the calculation can avert different assaults. The suggested framework is quick in execution and having an extremely straightforward calculation with less equipment unpredictability and less calculation overheads. It delivers an equivalent estimated figure content. The suggested approach is a novel document free enciphering plot where both the message record and in addition the key document is picked by the client itself.

7. REFERENCES

[1] Aswin Achuthshankar, Aswathy Achuthshankar," A Novel Symmetric Cryptography Algorithm for Fast and Secure Encryption", 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)

[2] Abumuala. M, Khalifa. O and Hashim. A.-H.A, "A new method for generating cryptographically strong sequences of pseudo random bits for stream cipher", IEEE Int. Conf. on Computer and Communication Engineering (ICCCE), May 2010.

[3] Lin Ding, Chenhui Jin, Jie Guan and Qiuyan Wang, "Cryptanalysis of lightweight WG-8 stream cipher", IEEE Trans. on Information Forensics and Security, vol. 9, no. 4, pp. 645-652, Feb 2014.

[4] Lamba. C.S, "Design and analysis of stream cipher for network security", IEEE Second Int. Conf. on Communication Software and Networks, Feb. 2010.

[5] Sharif. S.O and Mansoor. S.P, "Performance analysis of stream and block cipher algorithms", IEEE Int. Conf. on Advanced Computer Theory and Engineering (ICACTE), Aug. 2010.

[6] Aissa. B, Nadir. D and Mohamed. R, "Image encryption using stream cipher algorithm with nonlinear filtering function", IEEE Int. Conf. on High Performance Computing and Simulation (HPCS), July 2011. [1]

[7] Wulandari. D, Kumala. A, Nugroho. S and Indarjani, S, "Comparison the insertion attack effects on randomness property of Dragon and Rabbit stream cipher", IEEE Int. Conf. on Computer, Control, Informatics and Its Applications (IC3INA), Nov. 2013.

[8] Zhou. J, Au. O.C, Zhai. G, Tang. Y.Y and Liu. X, "Scalable Compression of Stream Cipher Encrypted Images Through ConconcontextAdaptive Sampling", IEEE Trans. on Information Forensics and Security, vol. 9, no. 11, pp. 1857-1868, Aug. 2014.

[9] Feng Lifeng, Wang Xiaofeng and Fang Yingjue, "An Improved Algorithm of Stream Cipher Based on LFSR", IEEE Eigth Int. Conf. on Wireless Communications, Networking and Mobile Computing (WiCOM), Sept. 2012.

[10] Thi Hong Tran, Lanante, L., Nagao. Y, Kurosaki. M and Ochi. H, "Hardware Implementation of High Throughput RC4 algorithm", IEEE Int. Conf. on Circuits and Systems (ISCAS), May 2012.

[11] Weerasinghe. T.D.B, "An effective RC4 stream cipher", IEEE Eigth Int. Conf. on Industrial and Information Systems (ICIIS), Dec. 2013.

[12] Jian Xie and Xiaozhong Pan, "An improved RC4 stream cipher", IEEE Int. Conf. on Computer Application and System Modeling (ICCASM), Oct. 2010.

[13] Wai Wai Zin and Soe. T.N, "Implementation and analysis of three steganographic approaches", IEEE Third Int. Conf. on Computer Research and Development (ICCRD), Mar. 2011.

[14] Qian Yu and Zhang. C.N, "RC4 state and its applications", IEEE Ninth Int. Conf. on Privacy, Security and Trust (PST), July 2011.

[15] Ahmad. S, Beg. M.R and Abbas. Q, "Energy efficient sensor network security using Stream cipher mode of operation", IEEE Int. Conf. on Computer and Communication Technology (ICCCT), Sept. 2010.

[16] Kherad. F.J, Naji. H.R, Malakooti. M.V and Haghighat. P, "A new symmetric cryptography algorithm to secure e-commerce transactions", IEEE Int. Conf. on Financial Theory and Engineering (ICFTE), June 2010.

[17] Murugesh. R, "Advanced biometric ATM machine with AES 256 and steganography implementation ", IEEE Fourth Int. Conf. on Advanced Computing (ICoAC), Dec. 2012.

[18] Shukla, Rakesh Prakash, Hari Om, Bhushan, R.Phani, Venkataraman. S, Varadan and Geeta, "Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem", IEEE Int. Conf. on Machine Intelligence and Research Advancement (ICMIRA), Dec. 2013.

[19] Chao-Hsi Huang and Shih-Chih Huang, "RFID systems integrated OTP security authentication design", IEEE Int. Conf. on Signal and Information Processing Association Annual Summit and Conference (APSIPA), Nov. 2013.

[20] ByungRae Cha, HyungJong Kim and DongSeob Lee, "Design of New OTP System Using Homomorphic Graph by Changed Location and Angle of Fingerprint Features", IEEE Int. Conf. on Ubiquitous Multimedia Computing, 2008. UMC '08, Oct. 2008.

[21] ByungRae Cha and Sun Park, "Design and Efficiency Analysis of New OTP System Using Homomorphic Graph of Fingerprint Features", IEEE Int. Conf. on Convergence and Hybrid Information Technology, 2008. ICCIT '08, Nov. 2008.

[22] Eldefrawy. M.H, Alghathbar. K and Khan. M.K., "OTP-Based TwoFactor Authentication Using Mobile Phones", IEEE Eigth Int. Conf. on Information Technology: New Generations (ITNG), Apr. 2011.

[23] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo and Hoon Jae Lee, "Online banking authentication system using mobile-OTP with QR-code", IEEE Fifth Int.

Conf. on Computer Sciences and Convergence Information Technology (ICCIT), Dec. 2010.

[24] Borowski. M and Lesniewicz. M, “Modern usage of “old” one-time pad”, IEEE Int. Conf. on Communications and Information Systems Conference (MCC), Oct. 2012.

[25] Fengling Han, Jiankun Hu and Kai Xi, “Highly efficient one-time pad key generation for large volume medical data protection”, IEEE Fifth Int. Conf. on Industrial Electronics and Applications (ICIEA), June 2010.

[26] Matt. C. and Maurer U, “The one-time pad revisited”, IEEE Int. Conf. on Information Theory Proceedings (ISIT), July 2013.

[27] Jeyamala. C, GopiGanesh. S and Raman. G.S, “An image encryption scheme based on one time pads — A chaotic approach”, IEEE Int. Conf. on Computing Communication and Networking Technologies (ICCCNT), July 2010.

[28] Yan Zhang Chengqi Xu and Feng Wang, “A Novel Scheme for Secure Network Coding Using One-Time Pad”, IEEE Int. Conf. on Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09, Apr. 2009.

[29] Zhihua Chen and Jin Xu, “One-Time-Pads encryption in the tile assembly model”, IEEE Third Int. Conf. on Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008, Oct. 2008.

[30] W. Stallings, “Cryptography and Network Security”, fourth ed. Pearson Prentice Hall, 2006.