AN IMAGE BASED KEY GENERATION FOR SYMMETRIC KEY CRYPTOGRPAHY

G.Manikandan1*, S.Ramakrishnan 2, R.Rajaram 3, V.Venkattesh 4

1, 2 Assistant Professor, School of Computing,
SASTRA University, Thanjavur, India – 613401;
manikandan@it.sastra.edu, srk@ict.sastra.edu

3, 4 Student, School of Computing,
SASTRA University, Thanjavur, India – 613401;
rajsan.infotech@gmail.com, venkatkrish92@gmail.com

Abstract: **Information sharing through digital media is a vital and challenging one. Those challenges are addressed with the help of cryptographic and stenographic techniques. In general, strength of the symmetric key cryptographic algorithms is based on keys. The objective of this paper is to propose an approach to avoid image distortion due to transmission noise while transferring the image to the receiver for generating the key. For key generation a structure similar to alphabetical trie is used, which is generated from a unique character set. Triple DES algorithm is used for experimental purpose, which is well known for its block of randomized key bits based security and easy implementation.**

Keywords: Security, Symmetric key, Triple DES algorithm, Alphabetical trie, Dynamic keys.

I. INTRODUCTION

Cryptology is the study of techniques which ensures secrecy and authenticity of data. The two main branches of cryptology are cryptography, which deals with the study of design of such defending techniques; and cryptanalysis, which deals with the defeating study of finding loop holes to break such techniques, to recover information, or forging information that will be accepted as authentic. [1]

Framing a secret code, which is known only to the intended users and which makes the information unpredictable for the eavesdroppers is known as cryptography. Providing confidentiality to the information is the main goal of cryptography. Also providing authentication, integration, non-repudiation are also appreciable goals for it. In order to achieve these goals we need strong cryptographic algorithms.

Based on the key, the cryptographic algorithms are classified as symmetric key cryptography and Public key cryptography. Single key is used for encryption and decryption in symmetric key cryptography and in public key cryptography two keys are used by both sender and receiver where encryption is done using public key and decryption is performed using private key.

The rest of the paper is organized as follows. Second Section contains glimpses of cryptography; Third and Fourth section comprises of existing system and proposed system respectively. A case study and its stimulation are being explained in Fifth section. Finally in the sixth section the result is concluded.

II. LITERATURE REVIEW

In the year 2010, Lifang Wu et al., proposed a biometric cryptosystem for symmetric key cryptography based on face biometrics [2]. In this cryptosystem, a 128 bit bio-key is extracted by applying principal component analysis mechanism on face image. Since it is symmetric key cryptography, for retrieving the same bio-key at receiver side, the face image needs to be shared to receiver.

Krishnamurthy G.N et al., proposed a method to improve the Performance of Blowfish and CAST-128 algorithms using Avalanche effect in the year 2011[3].

An integrated block and stream cipher approach has been proposed by G.Manikanadan et al., for making the key more complex [5]. In this approach, the original key is first given to the blowfish algorithm for generating new key, and then the new key is taken as the key for RC4 algorithm for encryption. The encrypted message transferred to the receiver before the intruder knows the existence of block cipher for key generation. At the same time, the performance of stream cipher is not affected by this approach.

A Software tool has been proposed in the year 2011, which involves Cryptographic enciphering and deciphering using two different dimensional algorithms and also they are well assisted with File Splitting and Merging mechanisms [6]. It offers a good performance without compromising security and the performance is enhanced by modified F-function.

In the year 2012, G.Manikandan et al., has proposed a new approach for improving data security using blow fish algorithm iteratively [7]. In this approach, the sender when executes blow fish algorithm in iterations with single key, different cipher text is obtained for same plain text. So in this way data security is improved.

G.Manikandan et al., has proposed a software toolkit for increasing the key strength, in the year 2011 [8]. In this system, a technique called black box is introduced. In this black box technique, a fresh key is generated from the original key by doing some operations. So the intruder does not have any knowledge about existence of black box. So it is tough for intruder to break the key.

In the year 2012, G.Manikandan et al., has proposed an approach to generate dynamic keys [9]. In this approach, the dynamic keys are generated by using polynomial based key generation approach to avoid key distribution. Also the dynamic keys ensure the authentication and confidentiality in symmetric key cryptography.

III. PROPOSED SYSTEM

A biometric cryptosystem is proposed based on face biometrics. In this system, the sender needs the face image to be transferred with the encrypted message. So this system is vulnerable to transmission noise and brute force attacks.

We propose a new image based key generation algorithm, which generates dynamic and complex keys and avoids key sharing issues like transmission noise and brute force attack. Here we get the unique character set from the user, which appreciates the security of key by having a dynamic nature. The structure similar to the alphabetical trie is formed using the above unique character set, which appreciates the complexity of key. We choose a non-volatile image in public web sites, which avoids sharing of image to generate the key. Then the alphabetical trie formed using the unique character set, is applied on the chosen image. The block diagram of sender and receiver is shown in figure 1.a and figure 1.b.

A. Steps involved in the proposed system at the sender side is as follows

Step 1: Get the unique character set from user.

Step 2: Form the alphabetical trie like structure with the unique character set.

Step 3: Chose the non-volatile image in the public web site.

Step 4: Divide the image into row blocks based on the number of nodes in the above structure and columns into 26 blocks representing the alphabets.

Step 5: Then apply that structure on the divided image such that the each node will be mapped to an unique block on the divided image.

Step 6: Then calculate the mean values for the obtained intensity values in each mapped block.

Step 7: Then convert mean into binary bits, in which the mean values are represented with 8 bits, to generate the key.

Step 8: Then the generated key is given as input to the cryptographic algorithm for encryption with plain text to obtain cipher text.

B. Steps involved in the proposed system at the receiver side is as follows

Step 1: Get the shared unique character set from sender.

Step 2: Form the alphabetical trie like structure with the unique character set.

Step 3: Chose the same non-volatile image in the public web site.

Step 4: repeat steps from 4 to 7 as in sender side.

Step 5: Then the generated key is given as input to the cryptographic algorithm for decryption to obtain the plain text from cipher text.

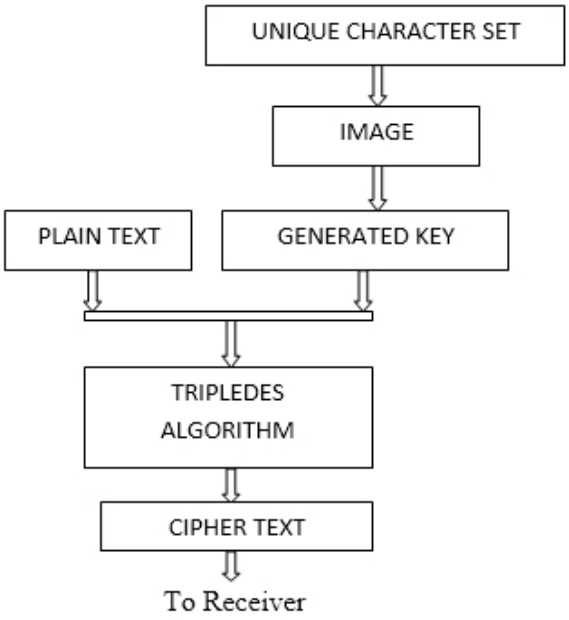

fig. 1.a

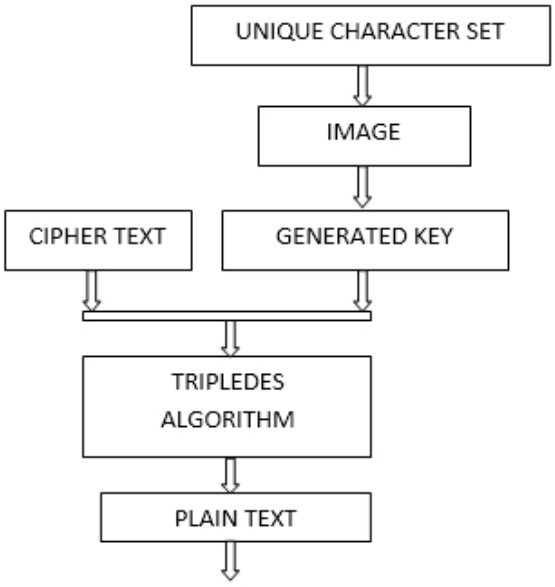

fig. 1.b

IV. CASE STUDY AND SIMULATION

For demonstration purpose, we form unique character set by concatenating date and day as shown in fig.2.Then the table is constructed using that formed unique character set, by taking number of charecters in unique character set as rows and constant 26 columns and form the trie like structure, as shown in fig.3.

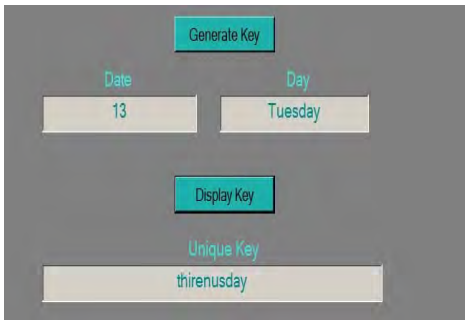

fig. 2

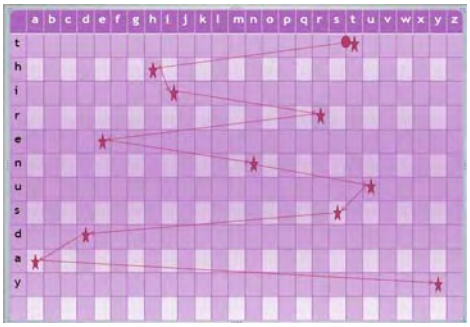

fig. 3

Then a non volatile image is chosen from public websites. For an instance, we choose an image as shown in fig.4. For demonstration purpose, the image shown in fig.4 is segmented into 26*26. Depending upon constructed trie, the segmented image is divided into row and column blocks. With reference to fig.3, there are 11 nodes in the constructed trie like structure. Then the image is divided into row block and column block as shown in fig.5. Here there are two sub rows and one sub column for each block as shown in fig.6. Because the trie like structure, with 11 nodes are to be mapped into the segmented image of size 26*26.

fig. 4

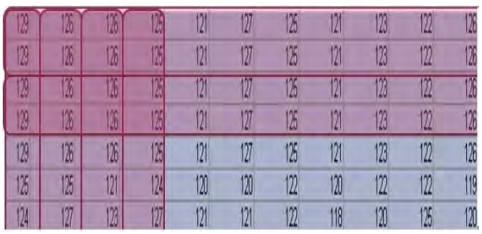

fig. 5

Then map the trie like structure with the segmented image. For example the first node t in trie like structure is mapped with respective column block twenty in the image, as shown in fig. 6. Then calculate the mean for obtained intensity values. Then do the same process for remaining nodes in trie like structure. So ‘n’ number of

mean values are obtained, where ‘n’ is the number of nodes in the trie like structure. Then number of key bits required is generated from the obtained ‘n’ number of mean values as shown in fig. 7. So while converting mean values into key bits, a mean value should be represented with eight binary bits minimum. Then the TripleDES algorithm is used for encryption and decryption. So a 192 bit key is generated, as shown in fig. 7, by replicating the 64 bit key obtained from mean values. Then the encrypted and decrypted file is shown in fig. 8 and fig. 9.

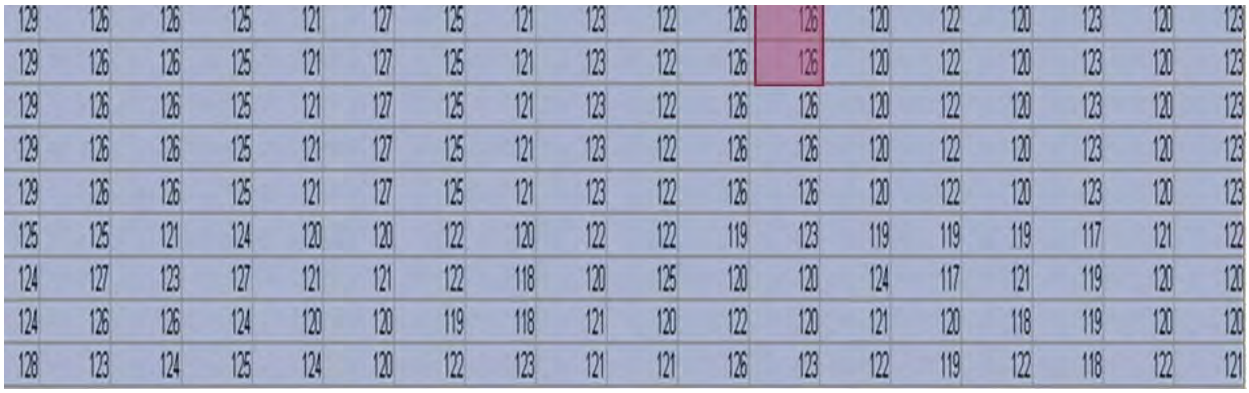

fig. 6

0001011101110110010111100000100000000111010010100111101000001011000101110111011001011110000010000000011101001010011110100000101100010111011101100101111000001000000001110100101001111010000010110001011101110110010111100000100000000111010010100111101000001011

fig. 7

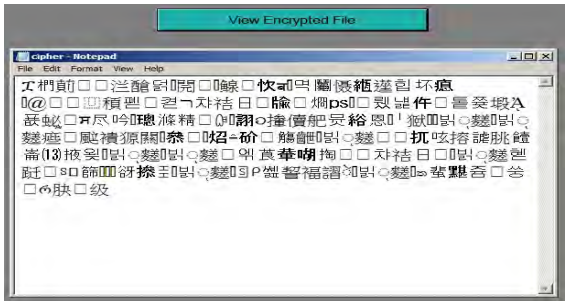

fig. 8

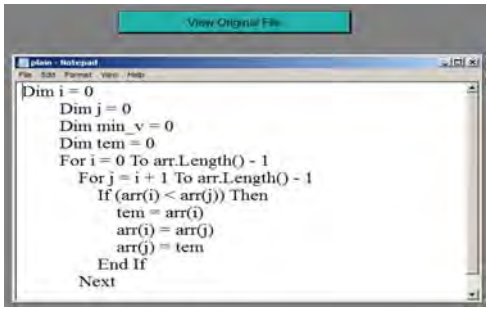

fig. 9

This approach is implemented in .net platform by using matlab, java and visual basic languages.

V. CONCLUSION

In this paper, we have proposed a new algorithm for key generation technique. The unique feature of the algorithm is that the key generated is dynamic in nature. In this approach, we have formulated a lookup table contains the image mapped using electronic code book combined with a unique character set for particular date and day. The non-volatile image is taken from the public websites and the unique character set is valid only for a day’s time. Thus this combined and dynamic approach of generating the key makes it untraceable and efficient.

REFERENCES

[1] William Stallings, Cryptography and Network Security, 3rd Ed, Wiley, 1995.
[2] Lifang Wu, Xingsheng Liu, Songlong Yuan, Peng Xiao, “A novel key generation cryptosystem based on face features”, Signal Processing (ICSP), IEEE 10th International Conference, 2010.
[3] Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E, “Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect”, IJCSNS 244 International Journal of Computer Science and Network Security, VOL.8 No.3, March 2008
[4] Andrew D.Gordon, Alan Jeffery, "Types and Effects for Asymmetric Cryptography Protocols", Journal of Computer Security, 2003, pp.1-48.
[5] G. Manikandan, R.Manikandan, P.Rajendran , G.Krishnan, G.SundarGanesh, “An Integrated Block and Stream Cipher Approach for Key Enhancement”, Journal of Theoretical and applied information Technology, June 2011.
[6] G.Manikandan, G.Krishnan, DR.N.Sairam, “A Unified Block and Stream Cipher Based File Encryption”, Journal of Global Research in Computer Science, July 2011.
[7] G.Manikandan, N.Sairam, M.Kamarasan,“A New Approach For Improving Data Security Using Iterative Blowfish Algorithm”, Research Journal of Applied Sciences, Engineering and Technology, 15 - March 2012.
[8] G.Manikandan, R.Manikandan, G.Sundar Ganesh , “A New Approach for Generating Strong Key in RC4 Algorithm”Journal of Theoretical and applied information Technology February 2011.
[9] G.Manikandan and J.Sivaguru “Dynamic Key Based Symmetric Cryptography", International Conference on Computing and Control Engineering, DR.M.G.R University,Chennai, April 12-13,2012.