Symmetric Key Generation Method using Digital Image

Ashraf Odeh[1], Aymen Abu-Errub[2], and Mohammed Awad[3]

[1] **Assistant Professor, Computer Information Systems Department, Faculty of Information Technology, AL Isra University, Amman, Jordan**

[2] **Assistant Professor, Part-Time Lecturer, Computer Science Department, KASIT, University of Jordan, Amman, Jordan**

[3] **Assistant Professor, Computer Science and Engineering Department, American University of Ras Al Khaimah, Ras Al Khaimah, United Arab Emirates**

Abstract

In this paper, the authors propose a new key generation algorithm based on using a binary image. The proposed algorithm converts 16×16 binary array representing the digital image into 4×4 array, then it converts the new generated array into 4×4 decimal array. The decimal array and the left diagonal of the original array are then used to generate the public key that is used to encrypt the data to be sent for the receiver. The proposed algorithm is also used in the receiver side to generate the private key used to decrypt the encrypted data.

Keywords: *Cryptography, Public Key, Private Key, Key Generation, Symmetric, Asymmetric.*

1. Introduction

Cryptography has been used for centuries to protect sensitive information and maintain the secrecy of transmitted messages. History indicates that since the days of the Romans and even in previous civilizations cryptography has been in use [1]. Nowadays, with the rapid technological advancement in the current Internet age, the importance in privacy is more than ever, people are interested in protecting their information for different reasons. This, in turn, has led to a heightened awareness of the need to secure data and resources from hacking and intrusion. Many lessons were learnt from the ignorance of security measures over Internet [2]. Now cryptography has become mandatory and it is considered a basic building block for the security of any computer system or network.

In the past, cryptography was mostly concerned about keeping the information confidential by using secret codes[1]. Nowadays, in addition to confidentiality, other cryptographic security services such as authentication, authorization, access control and integrity are quite common to provide security at different abstraction levels[2,3].

In this paper, we propose an algorithm to generate cryptographic key that will be eventually used to provide data confidentiality. Confidentiality is a service to maintain the contents of information accessible to only those authorized to have it. Encryption is performed on plain data to produce cipher data. The reverse process is known as decryption. An encryption algorithm or cipher is used to achieve confidentiality. A key is used during the encryption and decryption process. Encryption algorithms may be symmetric or asymmetric [4,5,6].

In symmetric key cryptography the same key (K) is used for both encryption and decryption as shown in Figure 1. The sender encrypts the plain data with key 'K' and sends the cipher data to the receiver through unsecured channel. On the other side, the receiver decrypts the cipher data, again using the same key 'K', back into its original form. The key should be kept secret and only shared via a secure channel between both the sender and the receiver.

Another kind of cryptography algorithms uses a key pair, one key for encryption (public) and the other (private) for

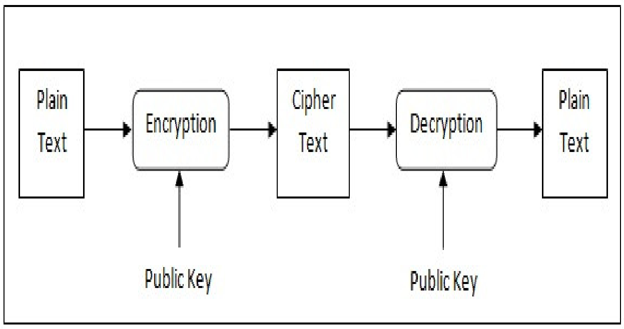

Fig. 1 Symmetric Key Encryption

decryption. These algorithms are called asymmetric key or public key algorithms. The encryption key, also known as public key, can be made public for anyone to do the encryption, but only the owner of the decryption key, also known as private key, can decrypt and read the cipher messages.

Figure 2 below, illustrates the asymmetric key encryption using key pair K1 (public key) and K2 (private key). Public key K1 can be made public and can be shared by many users through unsecured channel. Given a key pair, it is computationally, difficult to derive one key from the other; the difficulty depends on the size of the key [7].

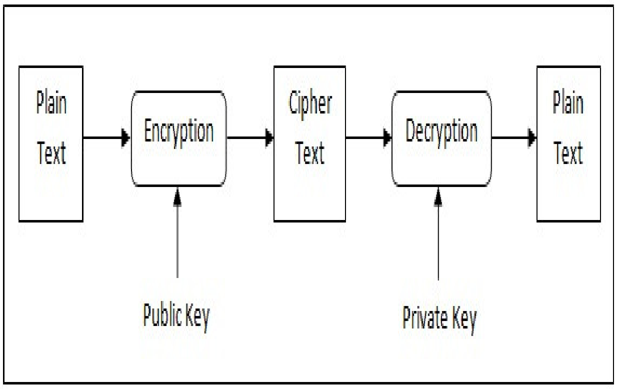

Fig. 2 Asymmetric Key Encryption

The asymmetric key algorithms are slower than symmetric key algorithms as they use large key sizes and complex mathematical functions for encryption and decryption.

For instance RSA public key algorithm uses l024-bit key and uses modular exponentiation and multiplication of larger prime numbers [2]. Public key algorithms are mainly used for authentication, key exchange, digital certificates and digital signatures. On the other hand, the symmetric key algorithms are used for high-speed bulk data encryption since they are fast as they use small key size.

1.1 Symmetric Key Encryption

As we mentioned earlier, symmetric key encryption uses the same key for both encryption and decryption as shown in Figure 1.

Most of the encryption algorithms are based on the following general principles [2]:

- Substitution: in which each element in the plaintext is mapped into another element.
- Transposition: in which elements in the plaintext are rearranged by means of shifts and rotate.
- Exclusive OR: in which elements in the plaintext are manipulated according to the truth table of XOR gate.

Many systems, involve a combination of substitutions, transpositions and, XOR transforms.

The rest of this paper is organized as follows: In Section 3, a brief overview of the related previous studies in which a number of researches that deal with key generation, encryption and decryption are presented. Section 4 illustrates the proposed algorithm. Section 5 presents the experiment and discuses its results. Finally, conclusions are provided in Section 6.

2. Previous Works

This section introduces a review of some related works that were previously published in key generation field.
Manikandan et. el. [8] proposed in there paper a key generation method based on image. The proposed method generates dynamic/complex keys and tries to avoids key sharing issues, (i.e. transmission noise and brute force attack). The first step of the proposed method is getting a unique character set from the user. Then an alphabetical tree like structure is formed using this unique character set. The authors choose a non-volatile image in public web sites to avoid image sharing to generate the key. To test their method, the authors formulate a lookup table containing a non-volatile image taken from a public websites and mapped it using an electronic code book combined with a unique character set for particular date and day. The authors claimed that their combined and dynamic approach of generating the key makes the generated key efficient and untraceable.

Srikantaswamy, and Phaneendra [9] presented in their paper an advanced encryption technique that combines both the features of substitution and transposition. Their algorithm uses five different key values; each one was used to substitute the corresponding plaintext characters in association with addition operation. The user of the algorithm first defined the basic key value, and then the next one is sets to be twice as of the previous one. The algorithm then uses a transposition technique that was employed by left shifting each bit of the tested data. The authors tested their algorithm and claimed that it provides an appreciable data security and requires minimum coding and involves less processing delay.

Solanki and Patel [10] tried to enhance the digital data security by introducing a biometric key generation method. The authors proposed a biometric key dependent cryptosystem in order to ensure the security of the system, they use fingerprint features as a key in a cryptosystem. The method extracts the features of the fingerprint and then generates a key using these features. The key is then used in digital signature to convert plain text into digital signature in asymmetric cryptography. The authors said that using fingerprint minutiae to generate a biometric key has produce an irrevocable and unique key, which can provides a better protection and replacement features for lost or stolen biometrics.

Jagadeesan et. el. [11], tries to integrate the volatility of the user's biometric features into the generated key, in order to generate key that is an unpredictable to hackers. In their paper, the authors proposed a new approach based on multimodal biometrics, iris and fingerprint, to generat a secure cryptographic key. Then the security of the key enhanced using the difficulty of factoring large numbers. The first step of the proposed algorithm is extracting the features of the fingerprints and iris images respectively. Then, a multi-biometric template is obtained by fusing the extracted features at the feature level. At the final stage the multi-biometric template is used to generate a 256-bit cryptographic key. The authors examine their algorithm using the fingerprint images obtained from publicly available sources and the iris images from CASIA Iris Database. The results of their experiments the generated key is capable of providing better user authentication and better security.

P. Balakumar and R. Venkatesan in their paper [12] use tow combined biometric features; fingerprint and iris to generate a cryptographic key. They begin their proposed method by extracting the fingerprints features; which needs to enhance the fingerprint image by normalizing, estimating the orientation, filtering and finally thinning the image. Then the minutiae features of the image are extracted, then they use mapping function to obtain the minutiae points, and finally, the lock/unlock data is extracted. Also the Iris features are extracted using localization and normalization process. Fusion process is then used on the four vectors obtained from previous step by shuffling, concatenating and merging of each individual feature vectors. The final process of the proposed algorithm is using the fused biometric features to generate the k-bit cryptographic key. The authors tested their algorithm on biometric features obtained from 100 persons. Then they used False Rejection Rate (FRR) and False Acceptance Rate (FAR) parameters to evaluated their algorithm. The authors claimed that the experimental result shows that their proposed algorithm results in better security than the existing techniques.

Sahu et. el. [13] proposed an encryption scheme used for large amounts of data using a new key generation algorithm. Their key generation algorithm is based on processing a digital image after dividing it into pixels. At the end of the process, the rms value of the image pixels is calculated and converted it into ASCII equivalence to generate the key that is used as the password of the encryption process. The authors claims that their proposed algorithm is characterized by many features such as loss-less image encryption, asymmetric public key encryption, and a reliable security.

A. Soni and S. Agrawal [14] proposed a new key generation method using Genetic Algorithm (GA). The proposed algorithm generates a random number using the system current date. The GA steps, crossover and mutation, is then applied on the generated pseudo random number to formulate a new number, which will be the secret key used for encryption. Symmetric key algorithm AES is used for encryption images process. The authors argue that their proposed algorithm will increase the efficiency of key generation because of reducing computation time and the robustness against hackers attacks.

3. Proposed Algorithm

The proposed algorithm consists of three phases. The first phase is generating the public key using a digital image. The second phase is using the generated public key to encrypt the data to be sent to the receiver. In the final phase the receiver uses the same key generating method to generate the private key in order to use it to decrypt the encrypted data.

Phase 1: Public/Private Key Generation

This section describes the method used to generate the public key which will be used in data encryption process, the same method will be used by the receiver to generate the private key that is used to decrypt the sent encrypted data. This phase is consists of 6 steps as described next, and as shown in the following figure 3:

1. Read the 16x16 bits binary image [A].
2. Group each 4x4 bits from array [A] into one element in a new 4x4 array [B] by concatenating each column and converting it to the equivalent decimal number.
3. Convert the original array [A] left diagonal into the equivalent decimal number and divide the resultant number by 16, the answer will be named (K).
4. Divide array [B] by the number (K) to generate array [B]'.
5. Find the sum of each row elements of array [B]' and put the results into new 1x4 array [C].
6. Concatenate array [C] elements to generate the public/private key.

IJCSI International Journal of Computer Science Issues, Volume 12, Issue 2, March 2015
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org

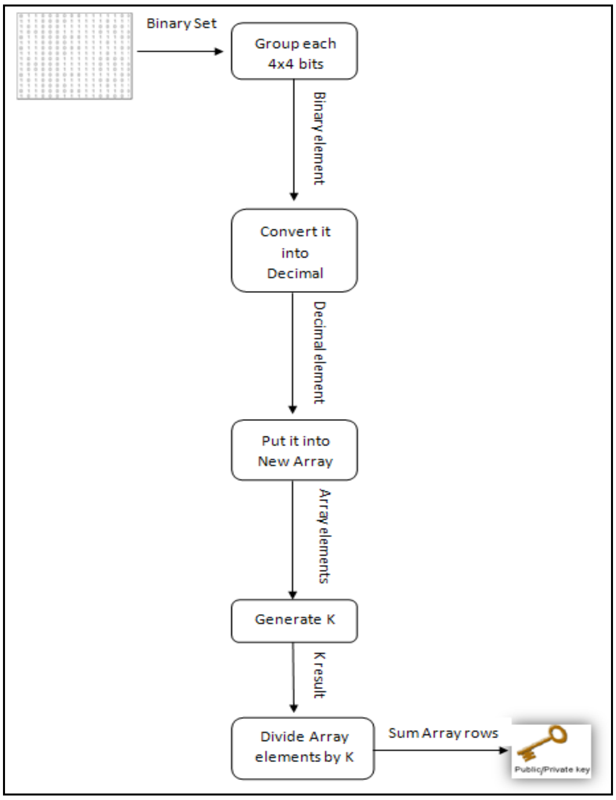

Fig. 3 Public / Private Key Generation Phase

Phase 2: Data Encryption Phase

This phase describes the data encryption method used by the sender to encrypt the data. figure 4. Shows the encryption phase steps:

1. Read the original data
2. Generate public key from image as in phase 1
3. Encrypt original data using public key generated in previous step.
4. Send encrypted data to receiver.

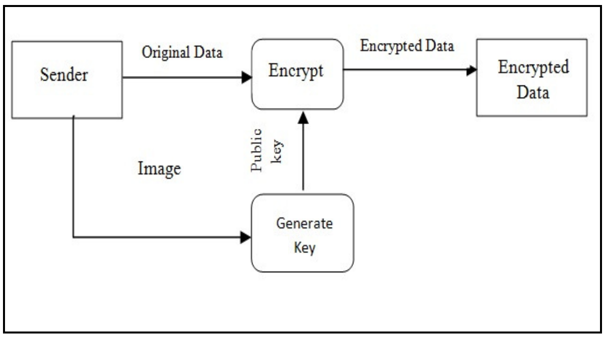

Fig. 4 Data Encryption Phase

Phase 3: Data Decryption Phase

The last phase of the proposed algorithm describes the steps of decrypting the received data. This phase uses the same key generation method used in phase 1 to generate the private key in order to use it in data decryption process. Figure 5 shows the complete steps:

1. Read encrypted data.
2. Read binary image sent by the sender.
3. Generate private key from the binary image as in phase 1.
4. Decrypt ciphered data using private key generated in step 3

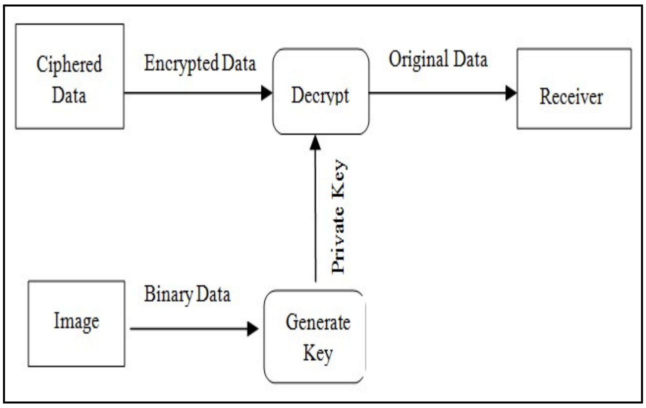

Fig. 5 Data Decryption Phase

4. Experiment and Results

The proposed algorithm was experimented using 16X16 bits binary images. Below are the experiment steps:

- Obtained the original binary image

0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1
1	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1
1	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0
1	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1

Fig. 6 Original 16X16 Binary Image

- Generating Array [B] from original Image

0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1
1	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1
1	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0
1	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1
1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1
0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0
1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1

14370	21214	14973	93106
10930	11409	10753	51522
78100	20156	71578	14861
11630	12093	11866	46211

Fig. 7 Generating Array [B]

- Array [A] left diagonal = 0110 1001 1111 0101
- Converting left diagonal to decimal = 27125
- Generating K = 27125 / 16 = 1695
- Dividing each element in Array [B] by K to generate array [B]'

8	13	9	55
6	7	6	30
46	12	42	9
7	7	7	27

Fig.8 Generating Array [B]'

- Generating Array [C] by adding each row elements in Array [B]

85
50
109
48

Fig.9 Generating Array [C]

- Generating the public/private key by concatenating array [C] elements (K) =481095085

4. Conclusions

In this paper the authors proposed a new algorithm to generate the public key used in encrypting data using a digital image. The proposed algorithm converts the digital image into a 16×16 binary array, and then the array is grouped into 4×4 binary array. The left diagonal elements of the original array are used to generate a unique number to use it in the final step of generating the public key. After using the generated public key to encrypt the data, the original image and encrypted data is sent to the receiver who will use the original image to generate the private key used to decrypt the encrypted data. The proposed algorithm was tested using various binary images and the results show the success of the algorithm to generate a robust and secure symmetric key that can be used for encryption process, with high complexity for being attacked by hackers.

References

[1] S. Singh, "The Code Book - The Science of Secrecy from Ancient Egypt to quantum cryptography", Anchor, 2000.
[2] W. Stallings, "Cryptography and Network Security - Principles and Practices", 3rd edition, Prentice-Hall, 2002.
[3] B. Schneier, "Applied Cryptography - Protocols, Algorithms and Source Code in C", Wiley, Second Edition, 1995.
[4] H.X. Mel, Doris M. baker and Steve Brunett, "Cryptography Decrypted", Addison-Wesley Professional, 2000.
[5] N. Ferguson and B. Schneier, " Practical Cryptography", Wiley, 2003.
[6] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, " Handbook of Applied Cryptography", CRC, 1996.
[7] T.Vladimirova, R. Banu, and M. N. Sweeting, "On-Board Encryption in Satellites", in the proceedings of the 8th Military and Aerospace Applications of Programmable Logic Devices and Technologies International Conference (MAPLD'2005), F-184, September 2005, Washington DC, US, NASA.
[8] G. Manikandan, S. Ramakrishnan, R. Rajaram, V. Venkattesh, "An Image Based Key Generation For Symmetric Key Cryptography", International Journal Of Engineering And Technology, Vol. (5) No. (3) P.P:2807-2810, 2013.
[9] S. G. Srikantaswamy, H.D. Phaneendra, "A Cryptosystem Design with Recursive Key Generation Techniques", International Conference on Communication Technology and System Design, Procedia Engineering 30, 170 – 173, 2011, Coimbatore, India, 2012.
[10] K. H. Solanki, Ch. Patel, "Biometric Key Generation In Digital Signature Of Asymmetric Key Cryptographic To Enhance Security Of Digital Data", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 2, February- 2013,
[11] A. Jagadeesan, T. Thillaikkarasi, and Dr. K. Duraiswamy, "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature", International Journal of Computer Applications, Vol. 2, Issue 6, Pp: 16-26, 2010.
[12] P. Balakumar and R. Venkatesan, " Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris", International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 201.
[13] A. Sahu, Y. Bahendwar, S. Verma, Prateek Verma, and Praveen Verma, " Proposed Method of Cryptographic Key Generation for Securing Digital Image", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, Pp: 285-291,2012.
[14] A. Soni, and S. Agrawal," Using Genetic Algorithm for Symmetric key Generation in Image Encryption", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, Issue 10, December 2012.

Ashraf Odeh is an Assistant Professor in Computer Information System at Isra University-Jordan. He received a BSc degree in

Computer Science in 1995 and MSc degree in Information Technology in 2003. With a Thesis titled "Visual Database Administration Techniques", He received PhD from department of Computer Information System in 2009 with a Thesis titled "Robust Watermarking of Relational Database Systems". He is interested in image processing, Watermarking, Relational Database, E-copyright protection, E-learning and E-content. He has submitted a number of conference papers and journals. Also he has participated in a number of conferences and IT days.

Aymen Abu-Errub is an Assistant Professor, he works as a part-time lecturer in computer science in King Abdullah II School for Information Technology, Unversity of Jordan, he worked for 5 years in the Faculty of Information Technology in Al-Ahliyya Amman University, Jordan in Computer Information Systems department, and then in Networks and Information Security department. He received his Ph.D. degree in Computer Information Systems from the Arab Academy for Banking and Financial Sciences, Jordan, in 2009. He has published several journal papers in information retrieval, information and networks security, and in risk management fields. He also participated and published his researches in scientific conferences.

Mohammed Awad is an Assistant Professor in Computer Science, he works in Computer Science and Engineering Department, American University of Ras Al Khaimah, Ras Al Khaimah, United Arab Emirates. He earned his PhD in Computer Science from the University of Houston in the United States in 2011. Dr. Awad’s research interest is in security issues, such as E-voting, and the security of the transmission of biometric data. He has published several journal papers in security fields, and he also participated and published his researches in scientific conferences.