Combination of Facial Biometrics and RSA Algorithms to Secure the Secret Message

Sayuti Rahman[1], Marwan Ramli[2*], Tommy[3], Ilham Faisal[4], Amru Yasir[5], Siti Sundari[6]
{masay.ram@gmail.com[1], marwan.math@unsyiah.ac.id[2], Tomshirakawa@gmail.com[3],
Ilhamoppa11@gmail.com[4], Cougara@gmail.com[5], Sundaristth@gmail.com[6]}

[1,3,4,6]Department of Engineering and Computer Universitas Harapan Medan
[2]Department of Mathematics, Universitas Syiah Kuala, Banda Aceh, Indonesia
[5] Department of Computer Management Universitas Dharmawangsa Medan, Indonesia

Abstract: This article describes the use of facial biometric features in implementing the security of digital messaging using RSA cryptosystems. Various studies have been conducted related to the security of secret messages one of which is RSA. The main focus on the RSA algorithm is the selection of public keys and private keys. Public key generation techniques as well as private keys can use simple random generation or other techniques such as using user biometrics like faces and other features. Cryptosystems that use facial biometrics require the identification process of the user face user involved, there are several techniques in recognizing the face one of them is to use back propagation algorithm because it is considered as a very stable algorithm in pattern recognition process but requires good preprocessing to be recognized by back propagation, prepossessing done with several stages of image processing that is gray scaling, then filtered with median, Otsu and split into grid to be input value to back propagation. By using face biometrics this app is capable of displaying messages according to user rights.

Keywords: RSA, Back propagation, biometrics, image processing, pattern recognition

1. Introduction

Today's technology is highly developed and facilitates various activities using computer devices. Increasing sophisticated network technology, both in the form of local network and internet, makes information easy to be obtained anywhere and anytime. The high value of information often causes many irresponsible parties to try to steal or manipulate information. The high security threats to information lead to the need for well-designed data security mechanisms by utilizing certain techniques or methods (A. Rai and S. Jain, 2017) in order to protect information from security threats in the form of theft and manipulation (Ashioba and Yoro, 2014)

Couple of study has been done in the field of message security which one of them is research on RSA method. RSA is a method that implements two keys namely public key and private key. Use of two different keys is expected to provide strong authentication validation so as to ensure the identity of the sender and recipient of the message. Key generators in the RSA are often developed with a variety of algorithms or key generator methods including the use of biometrics such as fingerprint (Rashid and Zaki, 2014) (Rahman, 2017), face, palm and other parts of the human body, that personally unique and have different features on every human being and there’s no need to memorized the key, but it needs additional process to identify the biometrics as the user's identity (Rahman and Ulfayani, 2017).

ICASI 2019, July 18-19, Banda Aceh, Indonesia

DOI 10.4108/eai.18-7-2019.2288570

This article utilizes features of facial biometrics as a key generator, where in some previous studies using fingerprint biometrics (Rashid and Zaki, 2014) there are still some disadvantages such as changes in fingerprint pixel values and orientation changes so that encryption and decryption processes often fail due to degradation or changes in the fingerprint image. Utilization of facial biometrics that implements back propagation has a better tolerance for less significant changes in the input image. The back propagation network has a very stable network in the pattern recognition process. The combination of facial biometrics and back propagation pattern identification can increase the success rate of the encryption and decryption process compared to the use of other biometric images that are more sensitive to changes such as fingerprints that are difficult to implement in the encryption and decryption process but for the use of facial biometrics it is still necessary pretreatment which is good to be well recognized by back propagation (S. Rahman, 2014).

2. Rsa Algorithm

RSA is also known as the asymmetric cryptography algorithm. The asymmetric cryptography algorithm is an algorithm that uses different keys for encryption and decryption processes. This algorithm is also called a common key algorithm because the key for encryption is made public or can be known by everyone, but the key to decryption is known only to the authorized person knowing the data is encoded or often called a private key (Rashid and Zaki, 2014).

RSA is the first algorithm suitable for digital signatures as well as encryption, and one of the most advanced in the field of public key cryptography. RSA is still widely used in electronic commerce protocols, and is believed to be secure by using keys that are long enough to make it difficult to decode.

RSA is an algorithm that involves expression with exponential function. The plaintext is encrypted in blocks, where each block has a binary value less than a certain number (n). The encryption and decryption process for plaintext block *M* and *C* block cipher text can be described as follows:

$$C = Me \bmod n$$
$$M = Cd \bmod n = (Me\ )\ d \bmod n = Med \bmod n$$

Sender and receiver must know the value of *n*. The sender knows the value of e and only the receiver knows the value d. Thus, it can be concluded that the public key of this algorithm is e, n and the private key is *d, n*. For the determination of this key is also not free, must be through a certain formula.

RSA algorithm security lies in the difficulty of factoring large numbers into prime factors. The generation of key pairs in RSA follows the following algorithm:

a) Select two primes, a and b (secret)
b) n = ab. Magnitude n need not be confidential.
c) m = (a - 1) (b - 1).
d) Select an integer for the public key, say its name e, which is relatively prime to m.
e) Calculate the decryption key, d, through ed≡1 (mod m) or (de) mod m = 1.

3 Back Propagation

Back Propagation is a gradient decreasing method to minimize the square of output error. There are three main stages including network training, namely forward propagation stage, step of propagation, and stage of weight change and bias, this network architecture consists of input layer, hidden layer, and output layer as in figure 1 [9].

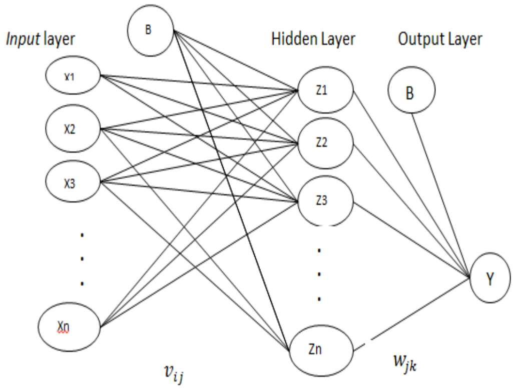


Fig. 1. Back Propagation Architecture.

Back Propagation Algorithms:

1. Weight initialization
2. Forward propagation.
3. Backward propagation
4. Terminated Stated.

5. Face Identification As Part Of Key Generation

The process of face identification requires a very long process, through the process of pre-image processing is grayscale, median filter to eliminate noise at the time of face capture, otsu used to get the best features available on the face image and grid is done to divide the image into 24 parts with each part possesses the frequency of occurrence of features in all parts of the pixel. The 24 values generated from this grid process are as input values on the backpropagation network. The result of some of these processes is stored in the training table, then from the training table is taken to be trained with the back propagation network, after the training weights are stored in the database, the application can recognize the faces entered, in this application takes the name of the face owner to get primes as public and private key generators on RSA. The process of face identification can be seen in figure 2.

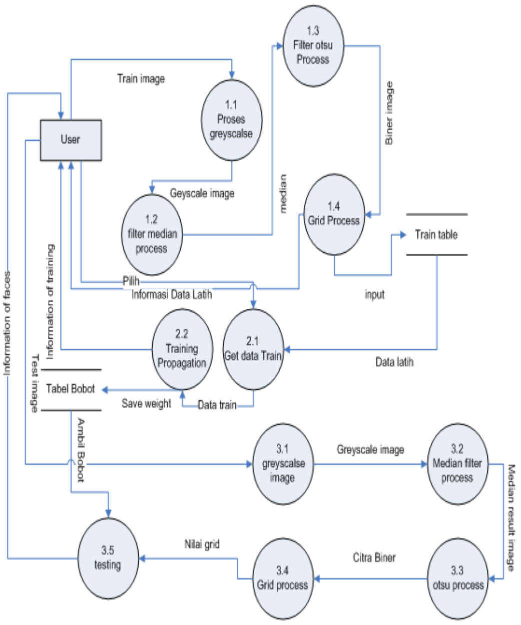


Fig. 2. Face Identification Flows.

The results from the process is the name of the face owner, suppose the face is inputted named "sayuti". The next challenge is to find the value of prime numbers to generate RSA keys, to be simpler then determined two pairs of primes for each face owner stored in the database.

To facilitate the calculation let the value of variables *a* and *b* is 11 and 7 then RSA key generation process steps as follows:

1. Calculate *n*, where n = *a* x *b.*
2. a = 11 and b = 7 then n = 77.
3. Calculate *m*, *m* = (*a* – 1) (*b* – 1);*m* = (11– 1) (7 – 1) = 0,
4. Then search e so GCD is 1.
   Nilai e = 2
   GCD (60,2) = 0
   Nilai e = 3
   GCD (60,3) = 0
   …
   Nilai e = 59
   GCD (60,59) = 1
   Obtained *e* = 59.
5. Calculate *d* where ed=1 (mod m) or (de) mod m= 1
   k = 1
   $d = \frac{(1+(1 \text{ x } 60))}{59}$
   d = 1.03
   k = 59
   $d = \frac{(1+(58 \text{ x } 60))}{59}$

d = 58
Because 58 is integer, then
d = 58

From above calculation we obtained n = 77 and e =59 as *public key* and d = 58 as *private key*. After the key pairs generated so encryption and decryption can be done with $C = P^e$ (mod n) and $P= C^d$ (mod n).

6. Implementations

Before the face can be recognized then it is necessary that the face data inputted into the system to be trained to obtain the weight of training stored in the database that will be used to identify the faces that are inputted on the next step that can be seen in Figure 3. The next processes are grayscale process, median filter, otsu and grid splitting before the feature stored in the database as shown in Figure 4.

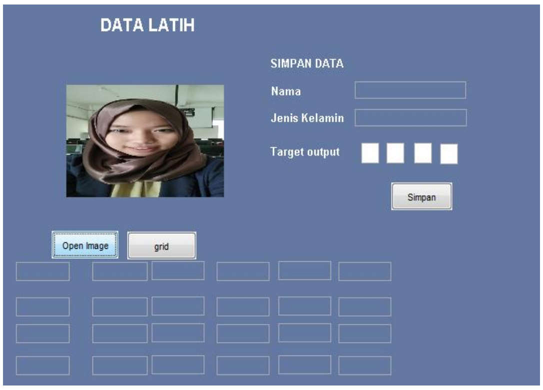
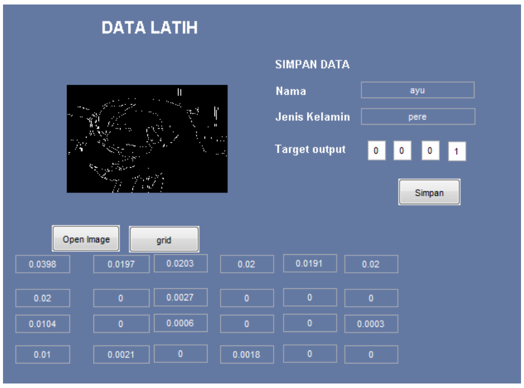


Fig. 3. Face Image.

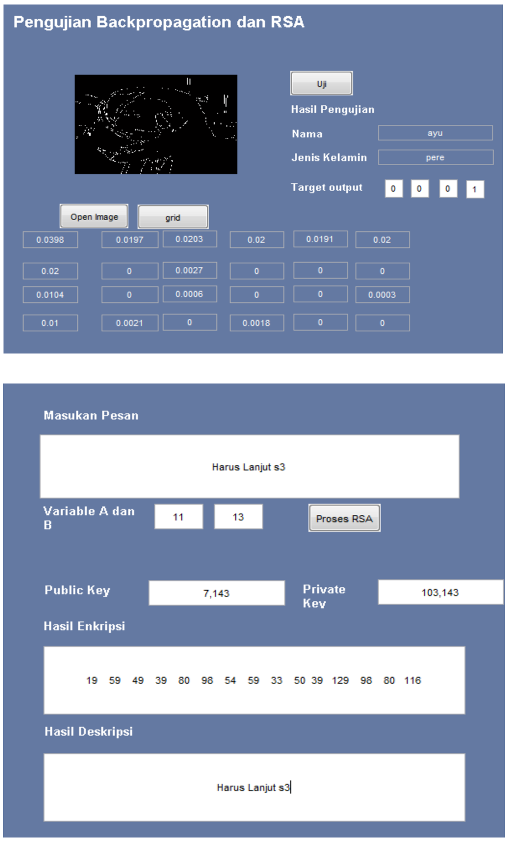


Nama: ayu
Jenis Kelamin: pere
Target output: 0 0 0 1

0.0398	0.0197	0.0203	0.02	0.0191	0.02
0.02	0	0.0027	0	0	0
0.0104	0	0.0006	0	0	0.0003
0.01	0.0021	0	0.0018	0	0

Fig. 4. Face Information.

After the stored process, back propagation network training process is done to get the training weight, after that the face can be used to generate RSA keys by calling prime numbers stored in the database according to the recognizable face.



Pengujian Backpropagation dan RSA

Hasil Pengujian

Nama: ayu

Jenis Kelamin: pere

Target output: 0 0 0 1

0.0398	0.0197	0.0203	0.02	0.0191	0.02
0.02	0	0.0027	0	0	0
0.0104	0	0.0006	0	0	0.0003
0.01	0.0021	0	0.0018	0	0

Masukan Pesan: Harus Lanjut s3

Variable A dan B: 11 13

Public Key: 7,143

Private Key: 103,143

Hasil Enkripsi: 19 59 49 39 80 98 54 59 33 50 39 129 98 80 116

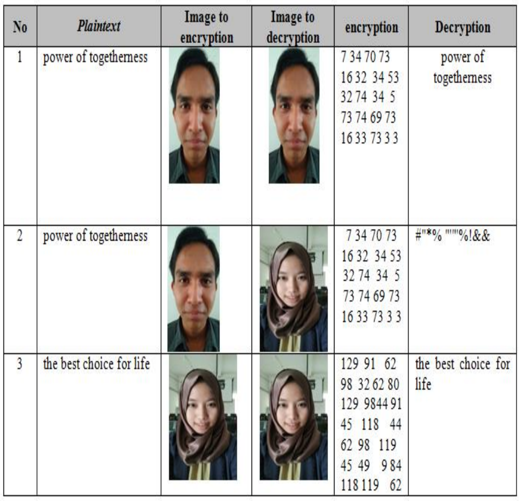
Hasil Deskripsi: Harus Lanjut s3

Fig. 5. Face Features as Key Generator.

7. Results

The implementation and testing was done using facial biometrics as the key generator where the results can be seen in table 1 below:

Tabel 1. Test Results.



No	*Plaintext*	Image to encryption	Image to decryption	encryption	Decryption
1	power of togethemess			7 34 70 73 16 32 34 53 32 74 34 5 73 74 69 73 16 33 73 3 3	power of togethemess
2	power of togethemess			7 34 70 73 16 32 34 53 32 74 34 5 73 74 69 73 16 33 73 3 3	#"*% """%!&&
3	the best choice for life			129 91 62 98 32 62 80 129 9844 91 45 118 44 62 98 119 45 49 9 84 118 119 62	the best choice for life

From table 1 above can be seen that the owner of a secret message encrypts a message with RSA using public and private key results from face recognition. And only the owner's face can see the original message. While viewing a message with a face other than the message owner will results false plaintext as the performance of this designed system is to use a face image trained with a back propagation network. Input on the back propagation network is a facial features that is extracted through a grayscale process, median filter, otsu filter and grid splitting to 24 parts. The feature was frequency value on each grid of face pixel occurrence on each grid as the back propagation network input data.

The features generated from preprocessing is stored in the database by adding data information such as the owner name and prime numbers are given from back propagation network training. The weight of the training results is stored in the database. The weight of this training result is used to recognize the face of the message owner, so that the encrypted message can be decrypted only by the message owner.

8. Conclusions

From RSA key generator design result using facial biometrics in message security, it can be concluded that:

1. Generating a key by utilizing the face image with back propagation method can be done well and become the key secrecy solution.
2. Face identification extraction is done by knowing the face owner and primes numbers stored in the database are used as RSA key generator.
3. Further research was need for the conversion of facial biometrics that is recognized immediately into the prime value that required on key generator.

References

[1] A. Rai and S. Jain (2017) '"Encryption and Decryption through RSA Cryptosystem using Two Public Keys and Chinese Remainder Theorem.', *Int. J. Comput. Appl.*, 170(1), p. 40–43,.

[2] Ashioba and Yoro (2014) ‘RSA Cryptosystem using Object-Oriented Modeling Technique.’, 4(2), pp. 57–61.

[3] Rahman, et. al. (2017) ‘Key Development Using Fingerprint Image.’, *J. Phys. Conf. Ser.*, 930 (1).

[4] Rahman and Ulfayani (2017) ‘Tangan Menggunakan Metode Freeman Chain Code,” CESS.’, *Journal Comput. Eng. Syst. Sci*, 2(2), pp. 64–73.

[5] Rashid and Zaki (2014) ‘RSA Cryptographic Key Generation Using Fingerprint Minutiae.’, *Iraqi Comm. Comput. Informatics*, 1(1), pp. 66–69.

[6] S. Rahman (2014) ‘Face Detection Menggunakan Robert Edge Detection dan Jaringan Back Propagation pada Citra Digital.’, *Snastikom*.