Biometric and Data Secure Application for Eye Iris’s Recognition Using Hopfield Discrete Algorithm and Rivest Shamir Adleman Algorithm

Dicky Nofriansyah*, Badrul Anwar, Mukhlis Ramadhan

1 Department of Information Technology, STMIK Triguna Dharma, Indonesia

Abstract

Artificial neural network (ANN) was used to identify the characteristics of the input iris is represented by the binary value. Input from these characteristics trained by discrete Hopfield neural network algorithm for the "recognized" or NOT. Eye’s iris can be used as an alternative to overcome the problems of privacy and data security because of the unique characteristics present in the iris itself. Texture of it, are unique to each person having a texture pattern is stable throughout life, even it left and right eyes of someone else having the same texture. Call was recognized if the output produced in accordance with the trend of network or proximity input pattern to a target pattern. Rivest Shamir Adleman (RSA) implements a public-key cryptosystem, as well as digital signatures. RSA is motivated by the published works of Diffie and Hellman from several years before, who described the idea of such an algorithm, but never truly developed it. Results from this study is that the system can recognize the characteristics of it in identify more precise and good degree of accuracy, and can distinguish the iris with each other.

Keywords: eye iris recognition; artificial neural networks; discrete Hopfield algorithm

INTRODUCTION

This research is about pattern recognition of eye’s iris based on Artificial Neural Network. Eyes are the human senses which serves to see an object. In the eyes there are several parts of one of them is sliced. Eye or iris that is part of the circle encircling the pupil. Characteristic textures are very detailed and unique to each person and remain stable can be analyzed to be identified so that it can be a valid system for example for attendance, population data collection and security systems. The main objectives of the research were as follow: 1) to recognize the characteristics of the iris using a neural network using Discrete Hopfield Algorithm and Data Secure using RSA Algorithm, 2) to produce software that can analyze the characteristics of Discrete Hopfield Algorithm and Data Secure using RSA Algorithm.

Eyes are the human senses which serves to see an object. In the eyes there are several parts of one of them is sliced. Eye or iris that is part of the circle encircling the pupil. Characteristic of textures are very detailed and unique to each person and remain stable can be analyzed to be identified so that it can be a valid system for example for attendance, population data collection and security systems as shown in Fig.1.

There are several physical and chemical elements that make up the eye. The eye is also heavily involved with the nervous system, which allows the brain to take in information from the eyes and make the appropriate decisions on how to act upon this information. The nerves must be kept in prime condition or the brain may start to receive false images, or you will not take in enough information to get an accurate perception of your environment.
PROBLEM STATEMENT
This study is focused to develop biometric system and data secure application using RSA Algorithm. Biometric system is a development of the basic methods of identification by using the natural characteristics of the human being as its base which includes the characteristics of the physiological and behavioral characteristics. Physiological characteristics are relatively stable physical characteristics such as fingerprints, facial characteristic, iris pattern, or the retina of the eye. While behavioral characteristics such as signature, speech patterns, or typing rhythm, in addition to having a relatively stable physiological basis, is also influenced by psychological conditions volatile. By using a system that can identify a person by relying unique characteristics present in the iris of the eye so that it can be used as a basis for the biometric system.

Biometric systems are a development of the basic methods of identification by using the natural characteristics of the human being as its base which includes the characteristics of the physiological and behavioral characteristics. Physiological characteristics are relatively stable physical characteristics such as fingerprints, facial characteristic, iris pattern, or the retina of the eye. While behavioral characteristics such as signature, speech patterns, or typing rhythm, in addition to having a relatively stable physiological basis, is also influenced by psychological conditions volatile.

Artificial Neural Network is a branch of computer science that artificial intelligence applied where processing paradigm can provide any information that is inspired by the biology of the nervous system cells, like brain that processes information. Many of the benefits provided from the application of artificial neural networks such as pattern recognition, identification characteristics, sounds, detection of counterfeit money, the military and others.

Discrete Hopfield network is a neural network-connected full (fully connected), namely that each unit is connected to every other unit and has a symmetrical. Discrete Hopfield network can be used to determine whether an input vector "recognized" or "recognized", so the Discrete Hopfield very good for pattern recognition objects in the image. RSA is a great answer to this problem. The NBS standard could provide useful only if it was a faster algorithm than RSA, where RSA would only be used to securely transmit the keys only. Thus, an efficient computing method of D must be found, so as to make RSA completely stand-alone and reliable.

SCOPE OF WORKS
A study was focused on the development of biometric system to pattern recognition using Discrete Hopfield Algorithm. The main focused of this research is to recognize of eye’s iris pattern. The biometric system is based on Artificial Neural Network. To used development Biometric System and analysis for recognition Eye’s Iris and combine with RSA Algorithm for keep data.

There are many differences of eye’s iris pattern. The iris is the area of the eye that contains the pigment which gives the eye its color. This area surrounds the pupil, and uses the dilator pupil...
muscles to widen or close the pupil. This allows the eye to take in more or less light depending on how bright it is around you.

ANALYSIS AND SYSTEM DESIGN
Discrete Hopfield network is a method that can be built in a system as a reading pattern in the iris of the eye. To read the pattern on this research using the artificial neural network like discrete Hopfield algorithm will change the image of the original image into a binary image. Capability using discrete Hopfield algorithm can actually recognize the image even if the pixels are not restricted, and is able to determine whether an input vector "recognized" or "NOT" by the network.

Called "recognizable" if output activation produced the same network with a vector that is stored by the network. Conversely, if the input vector "unrecognized" and the converged network generates a vector that does not constitute a pattern stored in a stable state of the network, it is called false (spurious stable state). Although in this study with all its limitations, still using discrete Hopfield algorithm simplest but it can resolve the issue specified.

This system is built to analyze the problems in the introduction of a person's identity using the iris as input data in the form of images. Where the image will be converted into binary form. The binary data will be processed by the Discrete Hopfield Algorithm, process characteristics of the iris recognition algorithm discrete Hopfield there are two main processes, namely the process of training and testing process. The output resulting from the application of the algorithm is the introduction of input and testing processes that have been previously entered. Discrete Hopfield Algorithm. The binary input pattern is the simplest of several branches of the network of discrete Hopfield neural network.

a. Selection algorithm a method with the cases studied is very important in the establishment of a system which is then developed and implemented in a system. In the process to picture image into a binary image that is worth matrix consisting of 0 and 1, the following are the steps: Input image of eye’s iris on 150 x 150 pixel (Fig.2)

![Fig. 2: Sampling Data](image)

b. Conversion into a binary image is processed by using Matlab.

```matlab
>> gbr=imread('iris matakananZulham1.jpg')
>> gray=rgb2gray(gbr);
>> thresh = graythresh(gray);
>> gbrBW=im2bw(gray, 0.3);
>> gbrInput = imresize(gbrBW, [20 20]);
>> imshow(gbrInput);
```

![Fig. 3: Data Converted](image)
Table 2: Binary Conversion of Figure

For a 20x20 pixel image that has been processed will produce binary values are used as an input image to be multiplied by the value matrix weight. For value is the weight matrix of 400 x 400 pixels. This is because the input image will be multiplied by the weighting matrix such as matrix multiplication matrix multiplier is the number of columns must equal the number of rows matrix. Initial weight W (a random value) 400 x 400. Bobot-symmetric weights (w$_{ij}$=w$_{ji}$; where I = rows and j = columns) with the main diagonal pattern 0. The input value is required as a vector. Dot product on input values obtained by altering the components of the vector with the weight vector W corresponding column / desired node and then add it.

Table 3: Value Matrix Weight (w)

Table 4: Result Value Activation Training

<table>
<thead>
<tr>
<th>Input</th>
<th>Node</th>
<th>Activation Value</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>11</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>14</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>15</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>17</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>18</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>19</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>20</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>......</td>
<td>......</td>
<td>......</td>
<td>......</td>
</tr>
</tbody>
</table>
Matrix calculation so that a predetermined weight will be in attachment 1 attachment to
the calculation of the activation, the value function and the output value in accordance with the
target it is proving successful network trained to call back pattern. Function threshold value
(thresholding function) determined that neural networks can produce patterns are as follows:
\[ f(t) = \begin{cases} 
1 & \text{if } t \geq \theta \\
0 & \text{if } t < \theta 
\end{cases} \]

Note:
- \( t \) = Activation Node
- \( \theta \) = Threshold Value

Here's a table of test results with different input but produce the same output with the
output that has been trained and the value of training resulted in the activation of the first node to
the node that to 400.

<table>
<thead>
<tr>
<th>Table 5: Result Value Activation Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>INPUT</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>......</td>
</tr>
</tbody>
</table>

The conclusions are that DISCRETE HOPFIELD Algorithm being designed will produce output in
accordance with the proximity of the input pattern
to the target pattern.

Notes:
- Hopfield network is said to be up to the maximum
  value if a particular pattern of steady redial. Iteration limit is usually quite one cycle after a
certain pattern called stably.

Regarding the weighting matrix initials:
- a. Set the weights on the main diagonal to 0, is
  considering provisions that fully connected
  network except to himself (Wij = 0; i = j, for i =
  rows and j = columns)
- b. Set weights than those located on the main
diagonal with arbitrary numbers such that the
resulting vector output exactly match the input
pattern. This requires the selection of weights carefully with attention to symmetry matrix
initial weight. Definition of symmetric here is
between the weight matrix with the transpose of the matrix of the same weight. To ensure that
\( W_j \) must be equal to \( W_i \) where \( i \neq j \).

And for the RSA cryptosystem, we first start off by generating two large prime numbers,
'p' and 'q', of about the same size in bits. Next, compute 'n' where \( n = p \times q \), and 'x' such that, \( x = (p -1) \times (q-1) \). We select a small odd integer less than \( x \), which is relatively prime to it i.e. \( \gcd(e, x) = 1 \). Finally, we find out the unique multiplicative inverse of \( e \) modulo \( x \), and name it 'd'. In other words, \( ed \equiv 1 \pmod{x} \), and of course, \( 1 < d < x \). Now, the public key is the pair \((e,n)\) and the
private key is \( d \).

Suppose Sender wishes to send a message (say 'm') to Alice. To encrypt the message
using the RSA encryption scheme, Bob must obtain receiver's public key pair \((e,n)\). The message
to send must now be encrypted using this pair \((e,n)\). However, the message 'm' must be represented
as an integer in the interval \([0, n-1]\). To encrypt it, sender simply computes the number 'c' where
\( c = m^e \mod n \). Bob sends the ciphertext \( c \) to receiver.

To decrypt the ciphertext \( c \), receiver needs to use her own private key \( d \) (the decryption
exponent) and the modulus \( n \). Simply computing the value of \( c^d \mod n \) yields back the decrypted
message \( m \). Any article treating the RSA algorithm in considerable depth proves the correctness
of the decryption algorithm. And such texts also offer considerable insights into the various
security issues related to the scheme. Our primary focus is on a simple yet flexible implementation of the RSA cryptosystem that may be of practical value.

REFERENCES


978-602-70570-4-3 © 2016 Published by ITP PRESS
DOI 10.21063/ICTIS.2016.1041
262


