Louis Savenien Dupuis Journal of Multidisciplinary Research 2022,1: 28-30
Doi: 10.21839/lsdjmr.2022.v1.73

Research Article

# Creating automatic passwords and patterns based on image processing from back hand wrinkles

**A. Maria***

*Computer Science, Loyola High School, Dar Es Salaam, Tanzania*

*(Received: July 29, 2021; Revised: May 25, 2022; Accepted: August 11, 2022)*
*Corresponding author: A. Maria (E-mail: mariasamy23@gmail.com)

**ABSTRACT**

Passwords, Patterns and Finger prints are a ubiquitous part of the present age. They are the keys to unlock our online profiles, bank accounts, mobile phones, iPad, opening money Box (safe) which is hosted across a plethora of websites and other electronic devices. With each of our profiles necessitating a separate password, it is not uncommon for people to need up to 50 passwords. Recent events have now seen hundreds to millions of passwords leaked in online, more than one hundred million LinkedIn logins and tens of millions of Twitter logins were made available on the darknet. This paper aims at proposing a novel objective approach which utilizes wrinkles on the back four fingers of the human to create patterns or passwords automatically using randomization by extracting the four fingers back wrinkles using sensors then merging all four fingers' wrinkles together and make the system to create pattern or password without known by the user or any human beings. Each and every time the same wrinkles group is detected it creates and changes new passwords. This cannot be known to anyone. This can be done through image enhancement and morphologic methods through wrinkle retrieval. We identify the pixels of the image of wrinkles and label them as letters for each and every pixel of a particular finger wrinkles and give decimal values from the ASCII table. We merge all four finger tables and start creating randomized patterns using Boolean Expression. The methodology is explained below.

**Key words:** Omponent, formatting, style, styling

## INTRODUCTION

We are trying to introduce new method of creating passwords and patterns. People are very clever in assuming and getting passwords as they tried level best to encrypt or decrypt. Especially the programmers know how to retrieve them; we have a big solution to this passwords hackings. The logic is very simple. We introduce Finger back wrinkles counting. Through CMOS sensor we take the image of finger back wrinkles are detected. Through the process of Image enhancement and Image morphology we detect the wrinkles line clearly and trying to identify the pixels. Using ASCII code, decimal and binary values. Finally we merge all tables with decimal values are letter and connect them randomly using programming.

## METHODS

### Binary Image

The back finger wrinkles are converted into Binary Images in order to see lines clearly through image enhancement method (IHM) it makes the line visible and clear. They are displayed as black and white. Numerically, the two values are often 0 for black, and either 1 or 255 for white as seen in picture (Figure 1).

### Image Morphology

Using Image Enhancement and Image morphologic we try to get pixels. Each and every pixel is calculated using ASCII code and converted into Binary. The process as follows.


**Figure 1:** Hand image.

### Pixel Calculation of Index Finger

#### *Before Morphological*

These wrinkles are taken from Index finger. Using enhancement technique the wrinkles are defined as lines which is seen clearly. These lines are converted into Morphologic image in order to get pixels (Figure 2).

It is the morphological diagram for index finger. We can use as binary image. All the white color circle indicated as 0 and filled blue color is indicated as using ASCII code we can

take values for filled blue color circle, so we take the value for letter B. so the calculation of the index finger as follows:

ASCII code for W = 87 decimal values

ASCII code for B = 66 decimal values

For Light Blue we have small letter b = 98 decimal values (Tables 1-3).

This process is repeated for all 4 fingers. The assumption as follows. The wrinkles images are converted into Binary Image and Morphological Form. We repeat the process for the other three fingers. The wrinkles are detected and converted into morphological images in order to get pixels as shown in the following figures. In the same way each pixel of the colour is assigned to Dark Blue (B) light blue is (b) and the white space is W. We fill the tables with letters and the corresponding decimal values from ASCII table. The decimal values will be converted into binary code. Each fingers pixel table is indicated with different colors. Using different Biometric methods we try to get the wrinkle lines very clearly. The pattern methods

**Table 1:** Pixel Representation of Index finger

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| W | W | W | W | W | W | W | W |
| W | W | W | W | b | b | W | W |
| W | B | B | B | b | b | B | B |
| W | B | B | B | b | b | B | B |
| W | W | B | B | b | b | b | b |
| W | W | W | W | W | b | W | W |

**Table 2:** Indicates the corresponding decimal values

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 87 | 87 | 87 | 87 | 87 | 87 | 87 | 87 |
| 87 | 87 | 87 | 87 | 98 | 98 | 87 | 87 |
| 87 | 66 | 66 | 66 | 98 | 98 | 66 | 66 |
| 87 | 66 | 66 | 66 | 98 | 98 | 66 | 66 |
| 87 | 87 | 66 | 66 | 98 | 98 | 98 | 98 |
| 87 | 87 | 87 | 87 | 87 | 87 | 87 | 87 |

From this table we can calculate the total number of pixel values Binary Value.

**Table 3:** Total Number of element or pixels = 6 x 8 = 48

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1010111 | 1010111 | 1010111 | 1010111 | 1010111 | 1010111 | 1010111 | 1010111 |
| 1010111 | 1010111 | 1010111 | 1010111 | 1100010 | 1100010 | 1010111 | 1010111 |
| 1010111 | 1000010 | 1000010 | 1000010 | 1100010 | 1100010 | 1000010 | 1000010 |
| 1010111 | 1000010 | 1000010 | 1000010 | 1100010 | 1100010 | 1000010 | 1000010 |
| 1010111 | 1010111 | 1010111 | 1010111 | 1010111 | 1010111 | 1010111 | 1010111 |

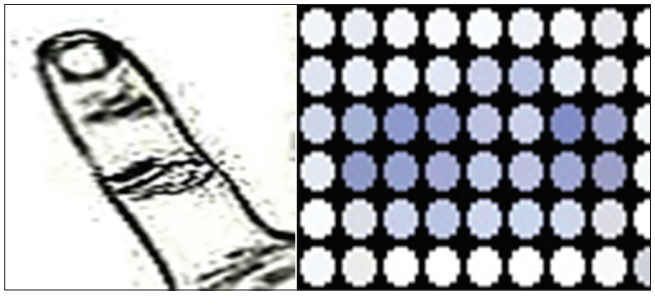


**Figure 2:** Index finger after Morphological.

can be created using Boolean Expression. It is clearly seen in Figure 3.

Now we connect all the wrinkle lines together with letter assigned for Randomizing. The four tables of Index finger, Middle finger, Ring finger and the baby fingers are put together. We make the possible patterns by using randomization.

The possible assumed patterns are:

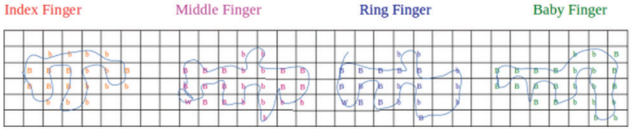
- Removing white space connecting all Capital B and small b
- Removing Capital B and connecting all small Bs
- Connecting All Capital B in table 1 and 3
- Connecting all Small b in table 1 and B in 3 tables.

Like that we can assume millions of way to create pattern. Passwords also can be processed from the table as follows
WbwB =87988766
BBWbb= 6666879898

The letters can be picked randomly and converted into decimal and binary. We can create millions of passwords (Figure 4).

Making Pattern by removing all white space (Figure 5).

Pattern Method 1:




Here we get 4 different patterns. The computer can choose as patterns.

Pattern Method 2:

Removing small letter b:


Pattern Method 2

Removing Capital Letter B:

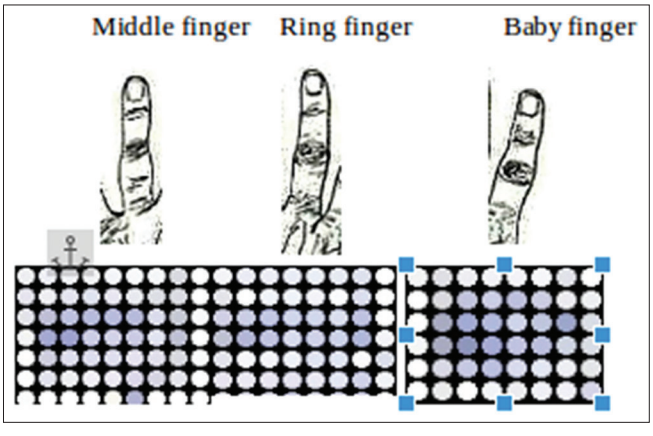



**Figure 3:** Merging all the wrinkles hexadecimal values.

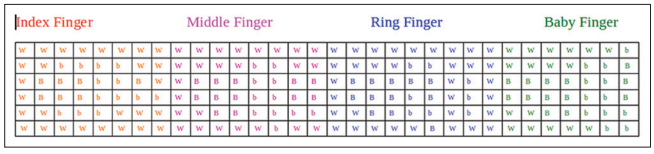
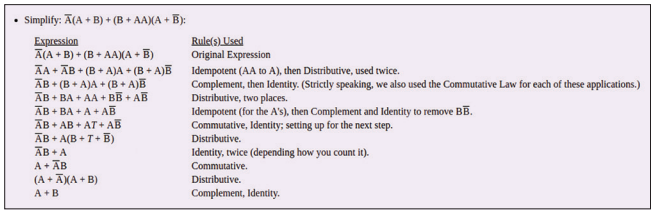



**Figure 4:** Assumed Randomized Patterns.


**Figure 5:** Pattern Methods.



- Simplify: $\overline{A}(A + B) + (B + AA)(A + \overline{B})$:

| Expression | Rule(s) Used |
|---|---|
| $\overline{A}(A + B) + (B + AA)(A + \overline{B})$ | Original Expression |
| $\overline{A}A + \overline{A}B + (B + A)A + (B + A)\overline{B}$ | Idempotent (AA to A), then Distributive, used twice. |
| $\overline{A}B + (B + A)A + (B + A)\overline{B}$ | Complement, then Identity. (Strictly speaking, we also used the Commutative Law for each of these applications.) |
| $\overline{A}B + BA + AA + B\overline{B} + A\overline{B}$ | Distributive, two places. |
| $\overline{A}B + BA + A + A\overline{B}$ | Idempotent (for the A's), then Complement and Identity to remove $B\overline{B}$. |
| $\overline{A}B + AB + A7 + A\overline{B}$ | Commutative, Identity; setting up for the next step. |
| $\overline{A}B + A(B + 7 + \overline{B})$ | Distributive. |
| $\overline{A}B + A$ | Identity, twice (depending how you count it). |
| $A + \overline{A}B$ | Commutative. |
| $(A + \overline{A})(A + B)$ | Distributive. |
| $A + B$ | Complement, Identity. |

**Figure 6:** Simplification of Boolean Expression.

Mathematical Pattern designing Using randomization. The following rules of Boolean Expression can be used for Pattern designing

Commutative Law

(a) A + B = B + A
(b) A B = B A

Associate Law

(a) (A + B) + C = A + (B + C)
(b) (A B) C = A (B C)

Distributive Law

(a) A (B + C) = A B + A C
(b) A + (B C) = (A + B) (A + C)

Identity Law

(a) A + A = A
(b) A A = A

Redundance Law

(a) A + A B = A
(b) A (A + B) = A
(a) 0 + A = A
(b) 0 A = 0
(a) 1 + A = 1
(b) 1 A = A

De Morgan's Theorem

(a) $\overline{(A + B)} = \overline{A}\,\overline{B}$

(b) $\overline{(AB} = \overline{A} + \overline{B}$

The pattern can be done with simplification of Boolean Expression (Figure 6).

In this simplification A+B can be joined and can be designed pattern or password only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A [m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

## CONCLUSION

People are very intelligent to crack password though it is encrypted in a complicated way. Children about 12 years started aiming at hacking. The hacker wants to access your online data by simply guessing your password; you're probably toasted in less than an hour. Now, there's more bad news: Scientists have harnessed the power of artificial intelligence (AI) to create a program that, combined with existing tools, figured more than a quarter of the passwords from a set of more than 43 million LinkedIn profiles. Yet the researchers say the technology may also be used to beat baddies at their own game. Here is small idea I have presented where people cannot know or assume or imagine each and anyone's password. The human beings can be easily found using their wrinkles though they switch off or change their simcards. I would like to introduce this method of protecting passwords we can reduce online theft.

## REFERENCES

https://www.techopedia.com/definition/26314/image-enhancement
https://www.cs.auckland.ac.nz/courses/compsci773s1c/lectures/ImageProcessing-html/topic4.htm
http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/FITZGIBBON/simplebinary.html
https://www.youtube.com/watch?v=EXZWHumclx0&t =171s
https://www.youtube.com/watch?v=QMLbTEQJCaI
https://www.youtube.com/watch?v=z1oySS7KHqs
http://www.sciencemag.org/news/2017/09/artificial-intelligence-just-made-guessing-your-password-whole -lot-easier