MODELING THERMAL SEQUENCE SIGNAL DECREASING FOR DUAL MODAL PASSWORD BREAKING

Duo Li⋆ Xiao-Ping Zhang† Guangtao Zhai⋆ Xiaokang Yang⋆ Wenhan Zhu⋆ Xiao Gu⋆

⋆ Institute of Image Communication and Information Processing, Shanghai Jiao Tong University, Shanghai, China
† Department of Electrical and Computer Engineering, Ryerson University, Toronto, Canada

ABSTRACT

The thermal camera records trace of users’ touch a while after they type in the password. People’s password may be stolen through a thermal camera due to this phenomenon. In this paper, we model the procedure of the thermal sequence from the viewpoint of physical process. Based on the Newton’s Law of Cooling, we set up a physical model to describe the process of the keys’ temperature decreasing. Then the model is used to estimate keystroke time instants by maximizing likelihood function method. We estimate the password after getting keystroke time instants of each key. The possibility that cheaters have to steal people’s password is also explored in the experiment. Based on our findings in the experiment, we give several pieces of practical advice for people to protect their password.

Index Terms— information security, infrared, multispectral, sequence analysis

1. INTRODUCTION

People are more and more careful about personal information protection in the modern time. However, there are many situations where people may suffer from security problem. Their personal information sometimes can be stolen by cheaters who use techniques with bad intentions. For example, in the internet, there are fake websites that seduce users to type in their pin code for credit cards. There are also hackers who steal millions lines of private records in public websites. Among information security problems, password cracking methods have been studied for many years [1][2][3][4][5][6].

Password breaking may occur in a physical way. Several researches explored different password breaking methods based on physical characteristics of the password input devices. These works have a strong correlation with the action of inputting passwords. In [1], the passwords of smartphone users are inferred by looking for pattern of oily residues on the screen. This work raises our attention of possible security problem caused by visible touch trace. In [2], the authors make use of signal from the smartphone integrated motion sensors. They designed an algorithm to infer user fingers’ move on the screen to estimate the graphical password. The correlated features do not only appear in smartphones, but also in ordinary password keypad. An interesting phenomenon has been found in [7]. In the website, the phenomenon of a thermal camera capturing people’s touch trace on the surface of objects is introduced. The possibility of password stolen is also mentioned. Thermal cameras can record the trace of touch on the keypads. As mentioned in [7], this may be used by cheaters who break people’s password for ATM machines, electronic lock safes, and alarm systems. In a recent study [8], authors have explored the probability that cheaters steal users’ passwords via observing users’ touching trace after users’ leaving. Inspired by [7], they have tested and verified that cheaters have a larger chance to steal the password with help of the thermal camera. There exists a large chance to recover the codes (ignoring the order) in the
password through the computer program to analyze thermal data.

Previous work on this phenomenon do not concentrate on the deep principle behind the presentation. In this paper, we propose a signal model to describe the procedure of thermal sequence signal decreasing after users’ touch on the keypad. Based on Newton’s Law of Cooling, we find that the signal decreases with a strict discipline. Through the model, we can study the characteristics of thermal attacks to design better coping strategies. We transform the problem of key touching time estimation into the least square problem. Due to thermal noise, the actual value of temperature on the surface of the keypad cannot be recorded. The least square problem helps to reduce the impact of noise to an acceptable degree. We explore the feasibility of thermal attacks to steal the users’ passwords. We also experiment on test videos captured in different situations, trying to find out competing solutions on this type of attacking. Finally, we give a few suggestions on password protection for users in their daily lives.

2. MODELING

To estimate the password after the user’s touch, we need to analyze the thermal value change for each of the keys on the keypad. So one major problem arises: how to depict the process of temperature decreasing for each key. The physical principle behind this phenomenon is the Newton’s law of cooling. When an object’s temperature is higher than that of surrounding materials, there will be a heat transfer from the object to surrounding materials. After user’s touch, the touched keys are of higher temperature than the atmosphere, which causes the heat transfer. The touched keys gradually cool down during the heat transfer process.

For the password estimation, the first step is to estimate the key touching time. An essential factor to estimate the key touching time is the method to fit temperature decreasing curve. We first set up the heat transfer model, then solve the problem of curve fitting based on this model. We model the procedure using this law and find that the temperature of user touched keys decreases in an exponential order. Due to measurement noise, there exists noise for the measured temperature. We first write down the equation for the measured temperature $T_i(t)$.

\[
T_i(t) = (T_i(0) - T') e^{-\frac{hR}{C_iM_i}} + T'
\]

where $h$ is convective heat-transfer coefficient, $R$ is the area of the key, $T'$ is the temperature of the atmosphere. Heat loss causes the temperature decrease of the key.

\[
dQ_i = -C_i \cdot M_i \cdot dT
\]

where $C_i$ is the heat capacity, and $M_i$ is the mass of the key. By solving this differential equations, we get the temperature change with time of the key:

\[
T_i(t) = (T_i(0) - T') e^{-\frac{hR}{C_iM_i}} + T'
\]

From Equation (3), we know that the temperature of touched keys decreases with time by exponential order.

3. METHODOLOGY

For each key, we estimate its touching time by fitting the temperature decreasing curve. Then, we sort the key touching time to get the final guess of the password.

3.1. Touching time estimation

Given the above heat transfer model, we can estimate the touching time based on the observed thermal data. For key $h_i$, we track the central temperature changes with time $T_i(t)$. According to Equation (3), the temperature decreases with exponential order. Due to measurement noise, there exists noise for the measured temperature $T_i(t)$.

\[
T_i(t) = (T_i(0) - T') e^{-\frac{hR}{C_iM_i}} + \beta_i + \epsilon_i
\]

where $\alpha_i$ is the rate that temperature of the key decreases. $\beta_i$ is the temperature of the key when it is untouched. $\epsilon_i$ is the thermal noise. The above equation can also be written as:

\[
T_i(t) = A_i e^{-\alpha_i t} + \beta_i = A_i e^{-\alpha_i t} + (T_i(0) - A_i) + \epsilon_i
\]

To estimate parameters $A_i$ and $\alpha_i$, we first write down the likelihood function for $T_i(t)$:

\[
P(T_i|\alpha_i, A_i) = \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(T_i(t) - A_i e^{-\alpha_i t} - (T_0 - A_i))^2}{\sigma_i^2}}
\]

where $\sigma_i$ is the variance of the noise $\epsilon_i$. For a series of observation $T_i = \{T_i(t_k), k = 1, 2, ..., K\}$, the overall likelihood function is:

\[
P(T_i|\alpha_i, A_i) = \prod_{k=1}^{K} P(T_i(t_k)|\alpha_i, A_i)
\]

\[
= \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\sum_{k=1}^{K} \frac{(T_i(t_k) - A_i e^{-\alpha_i t_k} - (T_0 - A_i))^2}{\sigma_i^2}}
\]
Algorithm 1 Password Estimation

1: By setting a threshold for temperature change (value of \( A_i \)) of each key, we pick out keys composing the password \( p_1p_2...p_H \).
2: Get \( \alpha_1, \alpha_2, ..., \alpha_H \) by calculating local minimum of Equation (8) using brute force method. Average \( \alpha_i \) for all the keys to get \( \alpha_{avg} \).
3: for \( p_i \) do
4: Estimate value of \( A_i \) for each key with help of the general \( \alpha_{avg} \) in step 1 using Equation (9).
5: Estimation \( \hat{\alpha}_i \) for each key given \( \hat{A}_i \) using brute force method.
6: Calculate time \( t_{i,touch} \) that the user touches \( p_i \) using Equation (10).
7: end for
8: Final guess of the password: sort all the touch time \( \{t_1, t_2, ..., t_H\} \) from long to short, and get the corresponding order of keys.

By minimizing the following equation, we get maximum likelihood estimation of the parameters \( A_i \) and \( \alpha_i \):

\[
\hat{A}_i, \hat{\alpha}_i = \arg \min_{A_i, \alpha_i} \sum_{k=1}^{K} (T_i(t_k) - A_i e^{-\alpha_i t_k} - (T_i(0) - A_i))^2
\]

Equation (8)

Since above equation is convex for \( A_i \), and non-convex for \( \alpha_i \), direct minimizing above equation leads to local optimization. The optimal value for \( A_i \) is formulated as follows:

\[
\hat{A}_i = \frac{\sum_{k=1}^{K} T_i(t_k)}{\sum_{k=1}^{K} e^{-\alpha_i t_k}} - 1
\]

Equation (9)

Given \( A_i \), estimation of \( \alpha_i \) is done in a brute force way. Brute force means to sample a number of candidate values for \( \alpha_i \) and try to find one value that minimize Equation (8). Directly applying brute force method is slow and easy to converge in local minimum. To avoid getting local minimum solution, we design the algorithm to estimate parameters \( A_i \) and \( \alpha_i \) within three steps. By setting a threshold for temperature change (value of \( A_i \)) of each key, we pick out keys composing the password. We assume the password is consist of \( H \) keys: \( p_1p_2...p_H \). From Equation (3)(4) we observe that parameter \( \alpha_i \) is only relevant to the material, mass, and area of the keys. So the value of \( \alpha_i \) for different keys have are close. We first roughly estimate each \( \alpha_1, \alpha_2, ..., \alpha_H \), then we average \( \alpha \) as to get \( \alpha_{avg} \). \( \alpha_{avg} \) is then used to estimate \( A_i \) for each key following Equation (9). Finally, we update the value of \( \alpha_i \) with help of \( \hat{A}_i \).

Having got the heat decrease function for each key, we can estimate the time that user’s finger touches the keys. Assume the key-touching time for the \( i \)th key is \( t_{i,touch} \), thus the corresponding temperature at \( t_{i,touch} \) should be equal to that of user’s finger (marked as \( T_u \)).

\[
t_{i,touch} = -\frac{1}{\alpha_i} \ln \frac{T_u - \hat{\beta}_i}{A_i} = -\frac{1}{\alpha_i} \ln \frac{T_u - T_i(0) + \hat{A}_i}{A_i}
\]

Equation (10)

In the algorithm, temperature of user’s finger \( T_u \) is measured in advance.

3.2. Password estimation

We assume that set \( \Gamma \) consist of all the combination of keys. Determine touching order of keys by sorting \( \{t_{i,touch}, i = 1, ..., H\} \), thus getting estimation of the password.

\[
p_1p_2...p_H = \arg \max_{h_1h_2...h_H \in \Gamma} P(t_{h_1,touch} < t_{h_2,touch} < ... < t_{h_H,touch})
\]

Equation (11)

In the experiment, we are given two chance to guess the password. Since the first two keys in the password are usually too close to determine the order, we exchange the them to generate the second guess.

4. EXPERIMENT

4.1. Experiment preparation

4.1.1. Benchmark algorithm

We compare with the benchmark algorithm proposed in [8]. For each key, benchmark algorithm calculate its temperature change in a single frame. Assume for key \( h_i \), the temperature is \( T_i(0) \). And the static temperature for the whole keypad is \( T_s \). Then the temperature change can be calculated as follows:

\[
T_i,change = T_i(0) - T_s
\]

Equation (12)

Then the password is estimated by sorting temperature change for all the keys \( h_1h_2...h_H \).

\[
p_1p_2...p_H = \arg \max_{h_1h_2...h_H \in \Gamma} P(T_{h_1,change} > T_{h_2,change} > ... > T_{h_H,change})
\]

Equation (13)

4.1.2. Experiment data

Our system contains two calibrated cameras: a RGB camera and a thermal camera. The RGB camera has a resolution of 720x1080, and the thermal camera has a resolution of 480x640. The two cameras are used to capture a image sequence after a user’s action to type in the password. Similar system structure can be found in [10][11]. In the RGB
Table 1. Accuracy of password guessing. For the metrics used in experiment, we count the percentage of correct estimation by first guess or first two guesses. When evaluating with two chances, there is a second chance to guess the password by exchange order of the first two keys.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Benchmark</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>One chance</td>
<td>6.67%</td>
<td>20%</td>
</tr>
<tr>
<td>Two chances</td>
<td>16.67%</td>
<td>30%</td>
</tr>
</tbody>
</table>

In the thermal images, tiny temperature change with time of objects’ surface are recorded.

We first locate the keys via the RGB camera. RGB camera is used to identify the keys’ corresponding position in thermal images. We use the SVM features to classify the numbers in binary form, which is implemented using OpenCV [12]. We analyze the thermal image sequences by tracking superficial temperature changes of each key. Locating keys in RGB images enables us to find the corresponding area to track temperature in thermal images.

Thirty pairs of videos are captured by aligned RGB and thermal cameras to verify effectiveness of the algorithm. The videos are captured shortly after subjects input the password with a length of 30 to 60 seconds. Air temperature is 25 degree centigrade. We also captured videos after conducting password protection methods. For each type of protection method, we captured ten pairs of videos. All the videos are captured within the same lighting condition.

4.2. Effectiveness

To compare the two algorithms, we test the thirty pairs of videos using both of the algorithms separately. We evaluate the algorithms using both one chance metric and two chances metric. One chance metric only count an estimation to be successful when first guess of the password matches ground truth. Two chances metric count gives the algorithm a second chance to guess the password. Experiment results are shown in Table 1. Our method outperforms the benchmark.

We select the first frame of each video as input of the benchmark algorithm. Fig 2 shows an example of the frame. The estimated password using benchmark algorithm is disordered among key 2, 3, and 6, because the temperature detected in this frame are disordered. The ground truth password is 672315, while the benchmark algorithm estimates 726315. The static temperature of each key is different, thus the absolute value of the key is not a robust feature to represent the touching order. Sometimes, there is a intersection of temperature before the thermal camera starts to capture, which makes the benchmark algorithm fails. The sequential analysis method proposed in this paper effectively avoids similar disorders, since dynamic method have the ability to aware the intersection.

<table>
<thead>
<tr>
<th>Action</th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrubbing</td>
<td>30%</td>
<td>10%</td>
</tr>
<tr>
<td>Blowing</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>Lowering light</td>
<td>30%</td>
<td>20%</td>
</tr>
</tbody>
</table>

Table 2. Accuracy of password guessing after using precaution actions

There may exist several ways to protect the password from being stolen using thermal cameras. Scrubbing the keypad after usage. Blowing to the keypad to cool it down quickly. Lowering the light of the keypad to obstruct the RGB camera to locate the keys.

We test the above three kind of actions. For each of them, ten pairs of videos are used for comparison test. The results are shown in Table 2. Scrubbing the keypad after usage seems to be the best and practical way to protect the password. Blowing the keypad to cool it down is hard to make sure whether it is enough for protection, though the accuracy is relatively lowered in the experiment. The action to lower the light receives effects to a certain degree, but this action also have an impact on user experience. The lighting condition is vital for the users to type in passwords. So the lowering light action is not a perfect solution.

5. CONCLUSION

In this paper, we study the phenomenon that the thermal camera records trace of users’ touch. By setting up a physical model to describe the process of the keys’ temperature decreasing, we estimate the password with higher accuracy. Based on the observation, we propose precaution actions to protect the password. In the future, we will do more research in designing better parameter estimation algorithm. The influence of surrounding conditions on password estimation is also an important problem, where we should pay more attention.
6. REFERENCES


