Color Space Conversion Based Texture Feature Model for Thermal Sequence Analysis

.M.Anithaarokiamary[1], S.Priyadharshini[1], Rajnandini Mali[1], Mrs.M.Premalatha.[2]

1,(Ug Student, Final Year Cse Department, Dhanalakshmisrinivasan College Of Engineering And Technology)
2(Professor, Department Of Computer Science And Engineering
Dhanalakshmi Srinivasan College Of Engineering And Technology)

Abstract: *The thermal camera can capture keyboard surface temperature change after human's touch. This phenomenon may be used to steal users' passwords physically. In this paper, based on the study of thermal dynamics of keyboards, we design a password break system using an infrared thermal camera. First, we build a signal model to describe the dynamic process of temperature change on the keyboard using Newton's law of cooling. Next, we develop a maximum likelihood parameter estimation algorithm to estimate the keystroke time instants. Then by maximizing the probability of key order arrangement, a novel password breaking algorithm is developed. Our algorithm is tested using simulated data as well as real-world data. Experiment results show that our algorithm is effective for physical password breaking using thermal characteristics. Based on our results, we discuss strategies for password protection at the end.*

Index Terms: *information protection, the rmal image, sequence analysis, password.*

I. Introduction

Personal computing devices now commonly use touch screen inputs with application-defined interactions that provide a more intuitive experience than hardware keyboards or number pads. Touch screens are touched, so oily residues, or smudges, remain on the screen as a side effect. Latent smudges may be usable to infer recently and frequently touched areas of the screen – a form of information leakage. This paper explores the feasibility of smudge attacks, where an attacker, by inspection of smudges, attempts to extract sensitive information about recent user input. In most cases it provide initial analysis of the capabilities of an attacker who wishes to execute a smudge attack. While this analysis is restricted to smart phone touch screens, specifically attacks against the Android password pattern, smudge attacks may apply to a significantly larger set of devices, ranging from touch screen ATMs and DRE voting machines to touch screen PIN entry systems in convenience stores.

KEYBOARD DEVICES

Keyboard is perhaps the most common human input device. In most cases we use keyboard to input a variety of information, some of which are highly valuable, such as passwords, PINs, social security numbers, and credit card numbers. It came as no surprise that keystroke logging is a favorite tool of trade by attackers. The attacker can install a Trojan program on the victim computer to log keystrokes, or use out of band channels to infer keystrokes. Acoustic key logger, for example, can infer keystroks from acoustic frequency signatures[2], timings between two keystroks[4], or language models[11].

Electromaganetic emanations of keyboards are also studied for keylogging [8]. Touch screen smartphones have changed the paradigm of user interaction. Most touch screen smartphones have no physical keyboard. Instead, the user types on the software keyboard on the screen. Since there is neither sound nor electromagnetic emanation from a virtual keyboard, the attacker can no longer infer keystrokes based on these signals. Moreover, many smartphone operating systems, such as Android and iOS, restricts privileges granted to applications. In most cases, an application cannot read keystrokes unless it is active and receives the focus on the screen.

IDENTIFICATION TASK

Currently, to read from the motion sensors, the key logging application needs to be installed on the victim smart phone. Given the increasing number of malware applications on the smart phone market [5] and the prevalence of potentially un-trusted third-party ad code incorporated in applications, we do not believe that this assumption is over-optimistic. The user also needs to grant the key logging application the privilege to read from motion sensors. We believe that most users would have no qualm of granting this privilege, as it seems much less risky than other sensor privileges, such as the microphone or camera. The assumption that most users would not treat motion data as highly sensitive is not just our wishful thinking.

Touch Logger
Pass word cracking
LOCAL BINARY PATTERN WITH GRAY SCALE INVARIANT

Let the gray value of the center pixel is gc and the gray values of the P circularly symmetric neighborhood with radius r is gp, where p=1, 2, 3, ……P-1.Now subtract gc from gp without losing the original gray information.

This gives the set ,

T= t(gc,g0-gc,g1-gc,g2-gc,……..gP-1-gc) (2)

Assuming differences gp-gc are independent of gc we can write

T≈ t(gc)(g0-gc, g1-gc, g2-gc, …….., gP-1-gc) (3)

Although an exact independence is not warranted; the factorized distribution is only an approximation of the joint distribution. However, we are willing to accept the possible small loss in information as it allows us to achieve invariance with respect to shifts in gray scale. The distribution t(gc) in equation (3) describes the overall luminance of the image, which is unrelated to local image texture and, consequently, does not provide useful information for texture analysis. Hence, much of the information in the original joint gray level distribution (1) about the textural characteristics is conveyed by the joint difference distribution

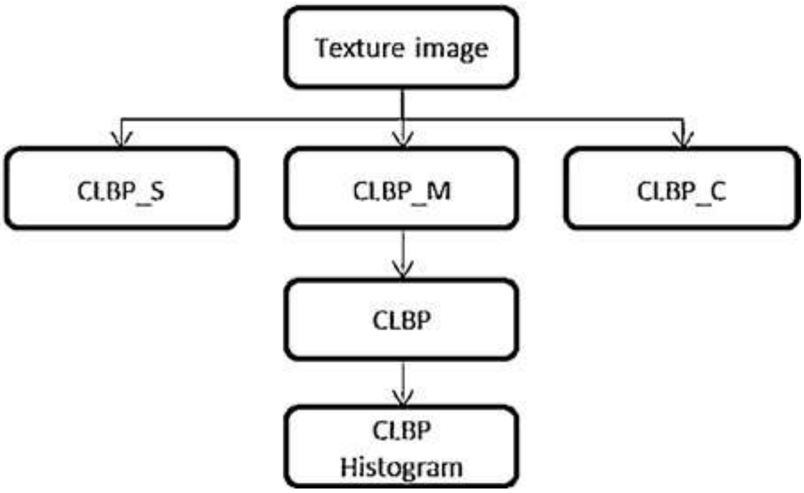


Fig. 1. CLBP.

PREPROCESSING:

A Lab color space is a color-opponent space with dimension L for lightness and a and b for the color-opponent dimensions, based on nonlinearly compressed CIE XYZ color space coordinates.The coordinates of the Hunter 1948 L, a, b color space are L, a, and b [1][2]. However, Lab is now more often used as an informal abbreviation for the CIE 1976 (L*, a*, b*) color space (also called CIELAB, whose coordinates are actually L*, a*, and b*). Thus the initials Lab by themselves are somewhat ambiguous. The color spaces are related in purpose, but differ in implementation. Both spaces are derived from the "master" space CIE 1931 XYZ color space, which can predict which spectral power distributions will be perceived as the same color, but which is not particularly perceptually uniform.

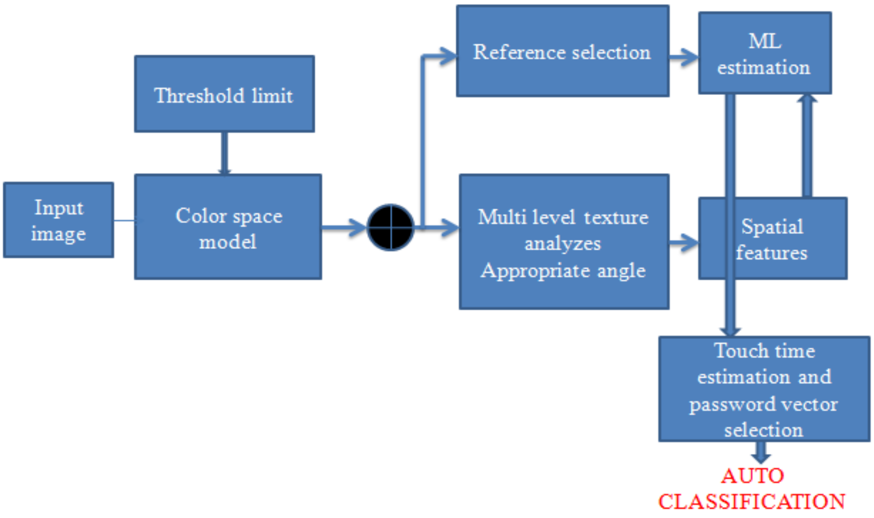
COLOR VALUE CONVERSION:

Strongly influenced by the Munsell color system, the intention of both "Lab" color spaces is to create a space which can be computed via simple formulas from the XYZ space, but is more perceptually uniform than XYZ. Perceptually uniform means that a change of the same amount in a color value should produce a change of about the same visual importance.CIE L*a*b* (CIELAB) is the most complete color space specified by the International Commission on Illumination (Commission International d'Eclairage, hence its CIE initialism).

It describes all the colors visible to the human eye and was created to serve as a device independent model to be used as a reference. When storing colors in limited precision values, this can improve the reproduction of tones. Both Lab spaces are relative to the white point of the XYZ data they were converted from. Lab values do not define absolute colors unless the white point is also specified. Often, in practice, the white point is assumed to follow a standard and is not explicitly stated (e.g., for "absolute colorimetric" rendering intent ICC L*a*b* values are relative to CIE standard illuminant D50, while they are relative to the unprinted substrate for other rendering intents) [3].

Unlike the RGB and CMYK colour models, *Lab* colour is designed to approximate human vision. It aspires to perceptual uniformity, and its *L* component closely matches human perception of lightness. It can thus be used to make accurate colour balance corrections by modifying output curves in the *a* and *b* components, or to adjust the lightness contrast using the *L* component. In RGB or CMYK spaces, which model the output of physical devices rather than human visual perception, these transformations can only be done with the help of appropriate blend modes in the editing application.

The three coordinates of CIELAB represent the lightness of the color (***L**** = 0 yields black and ***L**** = 100 indicates diffuse white; specular white may be higher), its position between red/magenta and green (***a****, negative values indicate green while positive values indicate magenta) and its position between yellow and blue (***b****, negative values indicate blue and positive values indicate yellow). The asterisk (*) after *L*, *a* and *b* are part of the full name, since they represent *L**, *a** and*b**, to distinguish them from Hunter's *L*, *a*, and *b*, described below. Since the *L*a*b** model is a three-dimensional model, it can only be represented properly in a three-dimensional space. Two-dimensional depictions are chromaticity diagrams: sections of the color solid with a fixed lightness. It is crucial to realize that the visual representations of the full gamut of colors in this model are never accurate; they are there just to help in understanding the concept. Because the red/green and yellow/blue opponent channels are computed as differences of lightness transformations of (putative) cone responses, CIELAB is a chromatic value color space.



FEATURE EXTRACTION:

Feature extraction in image processing is a technique of redefining a large set of redundant data into a set of features of reduced dimension. Transforming the input data into the set of features is called *feature extraction*. Feature selection greatly influences the classifier performance; therefore, a correct choice of features is a very crucial step. In order to construct an effective feature set, several published articles were studied, and their feature selection methodology was observed. It was noted that certain features were widely used as they gave a good classification. We implemented these features on *whole images* in our system.

II. Conclusion

In this paper, we present an attack that blindly recognizes input on touch screen from a distance. In this work, we also studied some camera-related vulnerabilities in Android phones for mobile multimedia applications. We also discussed the roles a thermal camera can play to attack or benefit attackers. In order discover several advanced thermal spot based attacks, including the remote- controlled real-time monitoring attack and types of pass code inference attacks we designed the template matching strategy to recognize the touched keys. We also use the texture models to detect touching keys. The GLCM matrix is derived by utilizing the intersections of the edges of the touch screen display. Our extensive experiments show that the first time success rate of recognizing touched keys is more than 90% while the second time success rate is more than 95%.Meanwhile, In the future, we will investigate the feasibility of performing spy camera.