Entropy of Graphical Passwords: Towards an Information-Theoretic Analysis of Face-Recognition Based Authentication

Stefan Rass, David Schuller, Christian Kollmitzer

Entropy of Graphical Passwords: Towards an Information-Theoretic Analysis of Face-Recognition Based Authentication

Stefan Rass[1], David Schuller[2], Christian Kollmitzer[2]

[1] Universitaet Klagenfurt, Institute of Applied Informatics, System Security Group, Universitaetsstrasse 65-67, 9020 Klagenfurt, Austria, stefan.rass@uni-klu.ac.at
[2] AIT Austrian Institute of Technology GmbH, Quantum Technologies, Department Safety & Security, Lakeside B01A, 9020 Klagenfurt, Austria, david.schuller.fl@ait.ac.at, christian.kollmitzer@ait.ac.at

Abstract. We present an information-theoretic discussion of authentication via graphical passwords, and devise a model for entropy estimation. Our results make face-recognition based authentication comparable to standard password authentication in terms of uncertainty (Shannon-entropy) that an adversary is confronted with in both situations. It is widely known that cognitive abilities strongly determine the choice of alphanumeric passwords as well as graphical passwords, and we discuss various selected psychological aspects that influence the selection process. As a central result, we obtain a theoretical limit to the entropy of a face-recognition based authentication in the light of some social engineering techniques (dictionary attacks on graphical passwords). Remarkably, our results hold independently of any information that can be obtained from the internet or through other forms of social engineering. Thus, we obtain very general bounds on the quality of authentication through face-recognition that solely depend on the authentication mechanism.

Key words: Graphical Passwords, Face-Recognition, Authentication, Shannon-Entropy

1 Introduction

Graphical passwords are an elegant way of overcoming a certain vulnerability of standard password authentication. A naive user may write down a password somewhere, or perhaps tell it on the phone, if an adversary manages to trick the user into believing that the call is from some honest service center. Composing an access code from images rather than symbols prevents writing it down, and also hampers giving the secret away otherwise. Using faces as images greatly supports memorability of the secret access code, and has therefore become a popular approach. Consequently, we consider face-recognition based authentication in the following, bearing in mind that the ideas presented here can easily be extended to various other types of graphical passwords (cf. the related work section).

A major contribution of this work is an information-theoretic measure of quality that a face-recognition challenge presents to the adversary. Since the quality of alphanumeric password policies can be measured in terms of entropy (using combinatorial considerations), an analogous measure for graphical passwords is certainly desirable. However, the literature about graphical passwords hardly provides any assertions about entropy of graphical passwords. It turns out that this goes much beyond the usual combinatorics that arises for standard symbolic passwords. In the case of face-recognition based authentication, such an entropy measure is, however, obtainable with combinatorial tools. The main task accomplished in this work is estimating the maximum possible entropy of an authentication challenge based on face selection. We demonstrate how to do this in section 3, along with a discussion of possible variations to the model. A further important point discussed in this work are psychological aspects regarding the memorability and selection process of images, particularly faces. Choosing weak passwords due to mental limitations of the human brain is a well-known problem. Similar concerns apply for some graphical password authentication systems, so choosing "weak face-sequences" is an equally likely incident. The second contribution of the paper is a discussion of such aspects, found in section 2.1. The paper closes with a small example illustrating the derived results, and discussing various directions of future research.

Related Work: The author of [1] gives various alternatives for alphanumeric passwords, along with discussions of security. The work of [2] contains vulnerabilities in face-recognition based authentication systems. An introduction to various kinds of graphical passwords is found in [3, 4] as well as [5]. The latter discusses the information content of (graphical) passwords in general, but does not provide specific upper bounds for the scenario we consider here. The authors of [6] present an implementation and empirical evaluation of a graphical password authentication system. Though entropy is discussed there briefly, a thorough formal analysis is missing. An interesting idea is given in [7], where graphical passwords are made resistant against spying over the shoulder of the user (shoulder-surfing). In [8], useful hints towards building a secure graphical password authentication system are found. We follow a similar path in this paper. Empirical studies regarding the performance of graphical passwords are given in [9]. Passfaces™[10], Déjà Vu [11] or Awase-E [12] implement authentication algorithms similar to the ones we consider here. We describe this mechanism in more detail in section 2. Other approaches to graphical passwords involve finding and clicking certain pass-positions within an image or drawing passwords on a grid. See [13] for further references.

2 Authentication through Face-Recognition

Face-recognition is one cognitive action that human brains are well accustomed to. Consequently, one would recognize faces easily, but describing a face to another person such that this face could too be recognized by the other person is

rather difficult. So why not use a sequence of faces (or general images) instead of a sequence of symbols for forming a password? This is the basic idea behind using faces for authentication: instead of being prompted to type in a password, the user is prompted to select a couple of faces from a pool of given pictures, with several decoy pictures among them (see [10–12]. In the sequel, we shall assume that the order in which these are chosen during the authentication is of no relevance (in section 3.3, we discuss how to account for this too). At the time when the "password" is chosen, the user is free to specify some images that will be recognized. This is completely analogous to choosing a password that can be remembered. For logging into the system, the user will pick the right ones among the decoy pictures to complete the authentication. The obvious advantage is that neither the faces can be written down, nor can easily be described to another person to permit that one to authenticate herself. In that sense, this approach appears superior to standard passwords, but a direct comparison is not trivial. For alphanumeric passwords, combinatorial considerations quickly lead to estimates how many passwords can be chosen according to the given policy. This can be taken as a measure of quality of the password-selection process. Can similar things be done for face-recognition based authentication? An answer is provided in section 3.1.

2.1 Psychological Aspects

We know that as early as the second and third days of life, babies are able to distinguish between happy and sad faces, by their second or third month they develop an affective consonance with their mother, to the extend that they reproduce more or less synchronized facial expressions [14]. It is true that these are most rudimentary forms of empathy, much less sophisticated than those underlying our social conduct when we reach maturity, but both require the capacity to understand the emotions of others, to read signs of pain, fear, disgust, and joy in their faces [15].

Empathy is the intimate and fundamental potential of socialization, however, there has been much controversy about the two main but contrastive theories over the last three decades which try to explain the ability to share emotions. The "theory of mind" argues that the development of other views and feelings can only be conceived with a previous knowledge or other outside appearances. It is defined by a cognitive determination individually given by experience. In the early 1990s, Giacomo Rizzolatti and his team discovered the mirror neurons and its location in the premotor cortex and partly in the cerebral cortex, which is responsible for the coordination of motion and also in the broca-areal which is responsible for the development of language. There are obvious reasons to define a connex between the mirror neurons an its location in brain areas that are indispensable for the ability to interact socially.

A critical review took place of how one is strongly contagioned by expressed emotions of others. These neurons seem to have the surprising property of responding not only when a subject performed a given action, but also when the

subject observed someone else performing that same action. Gallese, one of Rizzolatti's group members, speculated, that the mirror neurons enable a person to share intentions, views and goals. However, studies analyzing the correlation of language and the thinking of the state of mind of others question if the simulation mechanism fulfills also the ascription of emotions notionally. "This would mean that people with a damaged amygdala do not recognize fear in the faces of his fellow-men, nevertheless they often manage to see that fear anyhow," says Rebecca Saxe, a assistant professor at the Massachusetts Institute of Technology [15]. Other colleges see it differently. Claus Lamm from the University of Zurich [15]: "When we observe emotions it is primary about the symphatisation and not about the attribution of mindsets. Simulation theories employ emotions and actions, directly observable conditions, for example laughing or tears. "The theory of mind" generally examines the understanding of not directly observable conditions." Kai Vogeley from the University of Cologne says both sides are right. He differs between conscious thinking about others and prereflexive empathy, where we instantaneously understand others. In other words, the mirror neurons probably help us so we can intuitively emphasize with somebody, before we precisely form an imagination of the other person.

In times of growing media technologies an the insertion of attractive methods to capture clients, the image becomes more and more, what appears to be rated as a powerful expression to transfer emotions and action. In relation to our analysis of how people choose faces when they want to maximize security in internet operations we see how the levels of consciously clarifying expressions of others and intuitive immediate reactions to them mix together in various individual possibilities that appear to develop incomprehensibly. Though, if we look at social networking websites such as Facebook where users explicitly inform other users with illustrative material from their own livelihood and social backgrounds, we assume similarities between faceimages that are displayed (friends, admired movie stars, etc.) and faces that are picked for passcode identities, as we are constituted to refer to our images that represent our livelihood. These images are activators of emotive contexts that rely strongly on self-cumulative needs that want to be transferred in a interdependent form.

The exchange of selected pictures has become a prestigious way of socializing and the exclusion of images that could reveal own doubtful stories are commonly accepted. Therefore, pictures not reflecting on a specific individual coded cognition, are not chosen for safety-purposes. This fact may attract hacker, who inform themselves about such individual characteristic traits by looking at the images shown on personal websites. They can be looked upon as fairly reliable evaluations in order to raise the possibility to find security weaknesses. It is not yet clear if face-recognition systems do not have similar "weak spots" compared to passwords regarding the divulgement of the social surroundings behind published pictures of someone. Standard password dictionary used to go into other systems illegally are as imaginable for graphical passwords. With forty three muscles we can create more than ten thousand face expressions but only a few of them are seen regularly, foremost expressions that show our basic emotions

like fear or happiness. Unconsciously created Microexpressions may be a way of diminishing the vulnerability when choosing face images for authentication, as it is even more difficult to describe faces that seemingly express a "hidden look".

2.2 A Simple Dictionary Attack

Assume that the adversary has collected a pool of pictures that can be related to the subject whose graphical password should be identified. Such a pool can be constructed from social networking sites, such as Facebook (www.facebook.com), Twitter (www.twitter.com), MySpace (www.myspace.com) and many more; perhaps also photosharing websites like Flickr (www.flickr.com), for instance. A general purpose dictionary of pictures of people that are familiar to many persons may for instance be constructed using celebrity pictures that can be found via the image search feature of most of the popular search engines. A standard remedy against dictionary attacks are retry counters locking the login mask after a small numbers of failures.

It has been demonstrated that such sites can be exploited for automated social engineering [16], so using the same technology for collecting photos appears as an easy next step. A simple attack strategy is matching pictures from the login challenge screen with those in the dictionary. If strong similarities can be identified, then those pictures can be chosen for a trial login. If less pictures can be recognized than are in the dictionary, then the remaining ones have to be chosen on another basis; perhaps without any help in the worst case. Doing the matching is a challenge by itself, but can be done.

Many digital cameras sold nowadays are able to recognize faces quickly in order to properly set the focus of the camera. Such algorithms (see [17, 18]) can equally well be used for extracting faces from pictures of groups of people, or from pictures where the person is not the major content of the photograph. Several algorithms for matching pictures against each other are available in the computer vision literature (see [19]). Calculating similarity between images is a highly nontrivial task, as rotation (of the picture, as well as the person shown in the picture), can introduce severe difficulties. Nevertheless, similarity estimates *can* be obtained automatically, as has been demonstrated in the cited literature. We are basically concerned with the information-theoretic quality of passwords, leaving out the details of image processing here.

3 Entropy of Face-Recognition Challenges

In his seminal paper [20], C. Shannon introduced entropy as a measure of uncertainty of choices. In our case, this will be the choice of (password-)pictures from a given pool. Similarly as for alphanumeric passwords, where entropy measures the uncertainty of choice from the set of possibilities, graphical password selection too enjoys various degrees of freedom. Our model will upper bound the Shannon-entropy of the probability distribution modeling the selection of

a graphical password, thus yielding a natural measure of quality that is interpretable and comparable to standard measures. Before giving the model in section 3.1, we briefly introduce the entropy concept for convenience of the reader.

Shannon constructed the entropy H of a given probability distribution in order to satisfy three conditions [20]: First, H is nonnegative and continuous. Second, H strictly increases with the number of choices, if each of them is equiprobable. Third, if a choice can be decomposed into several sub-choices, then the overall entropy is the sum of the first choice's entropy, plus the weighted sum of each subsequent choice's entropies, where the weight is the probability of facing that choice. We will extensively use that property in section 3.1.

Shannon proved [20, Theorem 2] that the only function satisfying all three requirements is of the form $H(p_1, \ldots, p_n) = -K \sum_{i=1}^{n} p_i \log(p_i)$, with the convention that $0 \log 0 = 0$ and K being any positive constant. A common choice for K is such that the logarithm is to the base 2, giving the entropy in bits. We will implicitly assume this throughout the remainder of this work.

It is well known that entropy is maximized for the uniform distribution, in which case we have $H(1/n, \ldots, 1/n) = \log n$, and minimal for any degenerate distribution (i.e. point mass) making H vanish. To measure the quality of a password, one identifies the set from which those passwords are chosen, and calculates the entropy of the distribution from which the passwords are drawn. Doing some combinatorics to determine the number of possible passwords, the maximal uncertainty occurs of each of these is chosen with equal probability. However, this makes remembering the password an almost infeasible task. Using mnenomics or other tricks to easily remember or derive passwords changes the shape of the selection distribution into something different from the uniform distribution and thus lowers the entropy. If the same password is chosen by everyone, then there would be no uncertainty and hence zero entropy. Though counting the number of passwords and calculating the maximum possible entropy is often easy, determining the empirical entropy of passwords is a highly nontrivial task (see [21] for some figures). In this work, we shall take the first step for graphical passwords, leaving empirical studies subject of future research and follow-up papers. For existing field trials, see [9].

3.1 Upper-Bounding the Entropy

We seek a measure of uncertainty that resembles the way in which the quality of passwords is measured by Shannon entropy. Passwords are most easily remembered when they are words or somehow constructed from mnemonics. Following that idea, assume that memorability of faces is supported by drawing them from the pool of familiar faces in one's mind. Assuming further that many of those are available on social networking sites (Facebook, Twitter, etc.) or public photo-sharing (flickr.com, etc.). Let us introduce a probability for having chosen one face that the adversary could locate on the internet. This probability, along with the probability of actually having photographs on the internet, helps setting up a decision tree (cf. figure 1). We will upper-bound the entropy of the resulting probability distribution in the following, yielding a theoretical

limit of the entropy of graphical passwords, similar as this can be done for passwords. Throughout the remainder of this work, except where stated otherwise, we assume that the authentication system is insensitive to the order in which the faces (or images in general) are chosen by the user. This requirement can be relaxed, as we discuss in section 3.3. The variables for our model are as follows: n denotes the number of pictures that are found on the web and can be related to the subject of interest. p is the probability of the subject under attack having no personalized information (pictures) available on the internet. m is the number of pictures presented at the login-screen, and k is the number of pictures to be chosen for login.

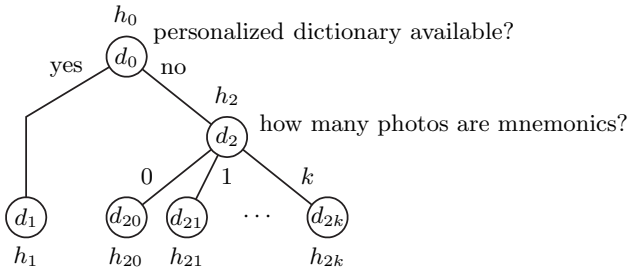

Fig. 1. Decision Tree

We give a step-by-step construction of the model, illustrating the idea using the decision tree displayed in figure 1. The first decision to be made is whether or not the subject under attack has pictures on the internet that enjoy a relation or some personal value. The decision d_0 has entropy h_0. If no, then we follow the left path, down to the face-recognition authentication with no additional information. The adversary gets a screen showing m pictures, k of which should be chosen. This choice d_1 has entropy h_1. Otherwise, if the internet does provide some personal photo albums or other pictures that can be related to the subject under attack, then how many of these have been used when the graphical password was chosen? Looking at decision d_2 (having entropy h_2), the user may have taken $1, 2, \ldots, k$ faces that looked familiar or are otherwise easily remembered. If none of the photos served as a graphical mnemonic (0), then the information from the web was worthless, and the entropy for the adversary is the same as h_1, making decision d_{20} basically identical to decision d_1. In each other case, we count the number of choices left to the adversary, and call the entropies $h_{21}, \ldots, h_{2k}$. We estimate each of these in the following, recursively combining them into an overall measure of uncertainty about the graphical password, in the light of "Web 2.0" [22].

Lacking precise estimates for the probability p, as well as the probability distribution on the set of decisions $\{d_{20}, d_{21}, \ldots, d_{2k}\}$, we can only search for some upper bound to the entropy. Unfortunately, it will not suffice to choose the

uniform distribution everywhere in order to maximize the overall entropy, as can be illustrated using the first decision d_0: fix h_1 and h_2 for the moment, then the worst case value for p is determined via the following optimization problem:

$$\begin{array}{rl} \text{maximize over } p: & H(p, 1-p) + ph_1 + (1-p)h_2 \\ \text{subject to} & p \in [0,1] \end{array}$$

The optimization goal can be simplified to $H(p, 1-p) + p(h_1 - h_2)$, discarding the constant additive term h_2. As H is differentiable, the optimal p is found by solving the equation $\frac{dH(p)}{dp} = h_2 - h_1$ for p within the range $[0, 1]$, giving

$$p^* = \frac{\exp(h_1 - h_2)}{1 + \exp(h_1 - h_2)}, \tag{1}$$

as the worst-case value for p. Though p is dependent on h_1, h_2, neither of them is dependent on p, so we are free to maximize h_1, h_2 separately. We start with a look at d_2 and its entropy h_2. Denote by $\pi = (p_0, p_1, \ldots, p_k)$ the probabilities for the events that $0, 1, 2, \ldots, k$ pictures have been found in the dictionary obtained through the internet. The entropy is found as $H(p_0, p_1, \ldots, p_k) + \sum_{i=0}^{k} p_i h_{2i}$, where $H(p_0, p_1, \ldots, p_k) \leq \log(k+1)$ with equality if π is the uniform distribution, and $\sum_{i=0}^{k} p_i h_{2i} \leq \max_i h_{2i}$ is trivial because a convex combination of values can never exceed the maximum term. The latter bound can be further explicated: suppose that i pictures have been found in the dictionary, then the remaining $k-i$ pictures are to be chosen from the given $m-i$ pictures on the login screen. Disregarding the order, this gives $\binom{m-i}{k-i}$ possible choices, so that $h_{2i} = \log \binom{m-i}{k-i}$ at most (again, using the fact that the entropy is maximal for the uniform distribution [20]). The recursive definition of the binomial coefficient through $\binom{m}{k} = \binom{m-1}{k-1} + \binom{m-1}{k} \geq \binom{m-1}{k-1}$, upon induction, instantly yields $\binom{m-i}{k-i} \leq \binom{m}{k}$ for all $i \geq 0$, so that $\max_i h_{2i} = h_{20} = h_1 = \binom{m}{k}$. Combining the bounds gives

$$h_2 = H(\pi) + \sum_{i=0}^{k} p_i h_{2i} \leq \log(k+1) + \log \binom{m}{k}. \tag{2}$$

Regarding h_1, a much simpler consideration tells us that without any dictionary of pictures, we are left with a choice of k pictures from a given set of m pictures at the login. This gives $\binom{m}{k}$ choices, and the entropy h_1 satisfies $h_1 \leq \log \binom{m}{k}$. Plugging the last inequality as well as (2) into (1) gives (after simplifying) $p^* = \frac{1}{k+2}$, as the worst-case value for p. Combining the maximal values into an overall upper bound for the entropy, we find that

$$\begin{aligned} H(p^*, 1-p^*) + p^* h_1 + (1-p^*)h_2 \; &= H\left(\frac{1}{k+2}, 1 - \frac{1}{k+2}\right) + \frac{1}{k+2} \log \binom{m}{k} \\ + \frac{k+1}{k+2}\left[\log(k+1) + \log \binom{m}{k}\right] &= \log\left[(k+2) \cdot \binom{m}{k}\right], \end{aligned}$$

after some messy algebra. Concluding all this, let H_{pf} denote the Shannon-entropy of a face-recognition based authentication challenge, where k faces are

chosen from a set of m given images. Then

$$0 \leq H_{\mathrm{pf}} \leq \log \left[(k+2) \cdot \binom{m}{k} \right], \tag{3}$$

where the lower bound is sharp, because once the secret image sequence is known to the adversary, the entropy vanishes. The accuracy of the approximation is dependent on the true shape of the distribution π, as well as the probability p. Both can only be determined through field trials, and are in turn depending on what and how many social networking activities the subject participates in. Hence, giving representative figures on the degree of approximation is beyond the scope of this work.

The reader may wonder why the parameter n (the number of pictures that have been obtained from the internet) nowhere appears throughout the whole analysis. The parameter n would have affected the distribution π that we used during the investigation of h_2 above. The more pictures are available, the more likely it is that some picture may have reminded the user of a face used for authentication. Though the number n may enjoy strong influence on the distribution, its impact vanishes due to the maximization argument that we used. Concluding that larger dictionaries give better chances to succeed in the authentication appears correct, but interestingly, it has no influence on the overall maximum entropy of the authentication challenge. This makes inequality (3) particularly appealing, as its value is solely determined by the parameters of the authentication challenge, and does not hinge on any unknown quantities.

Notice that the bound (3) can only be attained if the pictures are chosen such that no personal photograph (obtained from social networking websites) would provide a clue to the adversary on what pictures are likely to be the right ones. Furthermore, the probability p of finding such pictures has been optimized to yield a worst case estimate, so the actual entropy may be lower.

3.2 Example and Comparison

The correct values of p and n are to be determined by empirical studies, being subject of current and future research. Fortunately, neither of them appears in the bound (3). Figure 2 displays the upper bound of entropy for the parameter ranges $k = 5, \ldots, 8$ and $m = 16, \ldots, 64$. This corresponds to login masks displaying a 4×4 through 8×8-matrix of faces, of which 5 to 8 pictures have to be chosen. The numbers printed within the contour plot indicate the entropy measured in bit.

Notice that inequality (3) is only an estimate, and does not account for any psychological aspects that may have led to different choices. Taking those into account means deciding upon some faces being more likely chosen than others. Mathematically, this is expressed by deviating from the uniform distribution to a more bell-shaped distribution (possibly multimodal). We took this into account when we asked for the maximum entropy in our previous considerations. The result we obtained is independent of empirical estimates, and as such can be

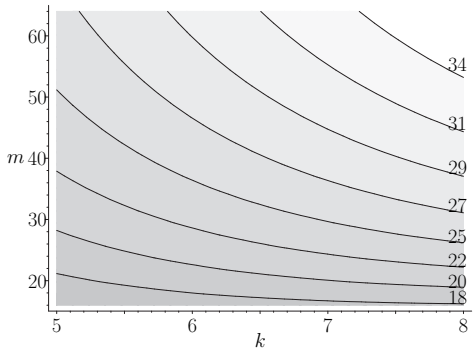

Fig. 2. Contour plot of entropy upper bound for various parameters k, m

taken as a theoretical limit to the power of face-recognition based authentication in terms of uncertainty for an adversary.

Let us compare the graphical face-recognition based authentication to a standard password authentication: assume that a password is chosen from the set of letters (case-sensitive), as well as numbers and 5 special characters. The password is required to contain at least 6 symbols, one of which must be a number, and one must be a special character. Doing the combinatorics, we find that the number of passwords with 6 characters is $N = 30226681500$, giving $\lceil \log_2 N \rceil = 35$ bit entropy at best (notice that the true value will be smaller due to mnemonics used to choose and correctly recall the password later). On the contrary, a face-recognition authentication challenge asking for 8 pictures to be selected from a 8×8-matrix on the login screen has about 34 bit of entropy at most. It follows that, in this example, passwords are still superior to the graphical password approach, because the entropy is most easily increased by different password policies (simply set the length to 8 characters with the same constraints to get more than 60 bit of entropy), while the face-recognition authentication enjoy less degrees of freedom to do that. One way out of this dilemma, however, is to make the authentication order-sensitive (i.e. the order in which faces are selected by the user matters), so that additional uncertainty is introduced. We consider this in future research, and briefly discuss the alter model below.

A standard PIN challenge (found at most ATMs) would ask for, say 5, digits out of ten, giving $\log(10^5) \approx 17$ bit of entropy. Doing the same with a face-recognition challenge presenting 25 images, 5 of which shall be selected, the entropy comes to ≤ 19 bit. The true advantage, however, is the resilience against shoulder surfing, because memorizing a PIN by looking over one's shoulder is much easier than memorizing a sequence of faces.

3.3 Variations of the Model

Inequality (3) can as well be used with more than a single source when we consider a joint source of pictures being composed of the websites that a user

most frequently visits. Such information can easily be obtained using Cookies, as is common practice.

Another interesting variation is achieved by letting the graphical password challenge account for the order in which the pictures are clicked by the user. This introduces additional uncertainty in the overall process, as even if some photos can be identified as similar to the given pictures, the order in which those are to be clicked remains unknown. The above calculations can straightforwardly be carried out by replacing the binomial coefficient $\binom{x}{y}$ by $y!\binom{x}{y}$, which accounts for the order too. In addition, to each h_{2i} (for $i = 0, 1, 2, \ldots, k$) one needs to add the uncertainty about the permutation, which is $\log(k!)$, if the graphical password is composed of k pictures.

4 Conclusion

We presented an information-theoretic approach to measuring the quality of face-recognition based authentication challenges. As being developed to be an alternative to standard password authentication, graphical passwords call for a measure of quality that make them comparable to standard authentication mechanisms. As it turns out, upper bounds to the entropy can be derived without empirical knowledge. The derivation of the upper bound (3) indicates that this one might be crude, and could be improved upon empirical studies. These in turn may lead to more complicated, but tighter bounds on the true quality of a graphical password authentication. Psychological aspects, such as discussed in section 2.1 are an important ingredient for constructing a more accurate model. Nevertheless, the theoretical limit (3) that we obtained here already indicates some limitations compared to standard password authentication. Considering the numerical results obtained above, an authentication asking for a selection of 8 pictures from a pool of 64 only has an entropy of ≈ 34 bit at best. However, this bound is only valid under worst-case assumptions, including that no personal photograph obtainable for the adversary gives any clues for the authentication challenge. As far as our results indicate, a face-recognition based authentication (in a simple form) is not an attractive alternative to standard passwords authentication.

References

1. Brostoff, A.: Improving password system effectiveness. PhD thesis, University of London, Department of Computer Science (2004)
2. Duc, N.M., Minh, B.Q.: Your face is not your password - face authentication bypassing lenovo - asus - toshiba. Technical report, Security Vulnerability Research Team, Bach Khoa Internetwork Security (Bkis), Ha Noi University of Technology, Vietnam (2009)
3. Eljetlawi, A.M., Ithnin, N.: Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods. Int. Conf. on Convergence Information Technology **2** (2008) 1137–1143

4. Suo, X., Zhu, Y., Owen, G.S.: Graphical passwords: a survey. In: 21st Annual Conf. on Computer Security Applications. (2005) 10 pp.+
5. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: SSYM'99: Proc. of the 8th conf. on USENIX Security Symposium, Berkeley, CA, USA, USENIX Association (1999) 1–1
6. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: Authentication using graphical passwords: effects of tolerance and image choice. In: SOUPS '05: Proc. of the 2005 symposium on Usable privacy and security, New York, NY, USA, ACM (2005) 1–12
7. Li, Z., Sun, Q., Lian, Y., Giusto, D.: An association-based graphical password design resistant to shoulder-surfing attack. IEEE Int. Conf. on Multimedia and Expo (2005) 245–248
8. Thorpe, J., van Oorschot, P.C.: Towards secure design choices for implementing graphical passwords. In: ACSAC '04: Proc. of the 20th Annual Computer Security Applications Conf., Washington, DC, USA, IEEE Computer Society (2004) 50–60
9. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords? a field trial investigation. In: Proc. of HCI 2000. (2000)
10. Real User Corporation: The science behind passfaces. Available at `http://www.realuser.com/published/ScienceBehindPassfaces.pdf` (September 2001) (last access: January 7th, 2010).
11. Dhamija, R., Perrig, A.: Déjà vu: A user study using images for authentication. In: Proc. 9th USENIX Security Symposium. (2000) 45–58
12. Takada, T., Koike, H.: Awase-e: Image-based authentication for mobile phones using user's favorite images. In: Proc. of the 5th Int. Symposium on Human-Computer Interaction with Mobile Devices and Services. Lecture Notes of Computer Science 2795, Berlin, Springer (2003) 347–351
13. Li, S., Shum, H.Y.: Secure human-computer identification (interface) systems against peeping attacks: SecHCI. Cryptology ePrint Archive, Report 2005/268 (2005) `http://eprint.iacr.org/`.
14. Rizzolatti, G., Sinigaglia, C.: Mirrors in the brain: How our minds share actions and emotions. Oxford University Press Inc., New York (2006)
15. Breuer, H.: Empathie – Streit um das soziale Hirn. Süddeutsche Zeitung (2010) p.16 (issue from the 4th of January).
16. Huber, M., Kowalski, S., Nohlberg, M., Tjoa, S.: Towards automating social engineering using social networking sites. In: 2009 Int. Conf. on Computational Science and Engineering (CSE). Volume 3., IEEE (August 2009) 117–124
17. Arnaud, E., Fauvet, B., Memin, E., Bouthemy, P.: A robust and automatic face tracker dedicated to broadcast videos. In: IEEE Int. Conf. on image processing, Genes Italy (2005)
18. An, K., Yoo, D., Chung, M.: An efficient fully automatic face tracking using binary template matching. In: Proc. of The Ninth Int. Symposium on Artificial Life and Robotics, Beppu, Japan (Jan. 28 30 2004) 37–40
19. Chen, C.H., ed.: Handbook of pattern recognition and computer vision. 3rd edn. World Scientific (2005)
20. Shannon, C.: A mathematical theory of communication. Bell System Technical Journal **27** (July and October 1948) 379–423 and 623–656
21. Yan, J., Blackwell, A., Anderson, R., Grant, A.: The memorability and security of passwords - some empirical results. Technical Report 500, University of Cambridge, Computer Laboratory (September 2000)
22. Wikipedia Foundation: Web 2.0. `http://en.wikipedia.org/wiki/Web_2.0` (2004) (last access: January 5th, 2010).