Reconfigurable Steganographic System with Hidden Double Layered Authentication

G. Margarov, V. Markarov, A. Khachaturov
Information Security and Software Development Department,
State Engineering University of Armenia,
105 Teryan str., Yerevan, 0009, ARMENIA
gmargarov@gmail.com, vmarkarov@yahoo.com, ashotian@gmail.com www.seua.am

Abstract - This work proposes a reconfigurable steganographic system offering mechanisms for secret sharing, reception of new and restoration of lost parts of the secret data, validity test for the parts of divided secret data, restoration of divided data employing a certain number of divided parts which provides long-term data storage. Finally this work introduces a mechanism for hidden double layered authentication, which hides the existence of steganographic system.

Keywords: Steganography, data hiding, secret sharing, graphical authentication, behavioral authentication, click point.

1. Introduction

Nowadays, due to the widespread availability of the Internet and other technologies, the threat of data loss, compromise or an attack on sensitive data located on the Internet, increases simultaneously. Security is an essential constituent of the process of incorporating new information technologies in all the spheres of social life. That is why wide-scale use of information and telecommunication technologies results in qualitatively and constantly evolving new possibilities of an unsanctioned access to the sources and data of various information systems, thus exposing them to ever growing threats and vulnerability.

Steganography is one of the most effective tools for protection of digital information. Modern steganographic systems provide features such as hiding secret data in visual images or in digital objects, which can be located on a local computer, in a local network or the Internet. The latter could be considered as the most appropriate environment for storage (and transfer) of secret data. The biggest downfall of this type of storage or transfer of secret data could be considered the risk of damaging or deleting steganographic files in the result of a targeted hostile attack or of ‘natural’ causes, e.g. such as closure or reorganization of the relevant web pages (mail boxes), etc. A solution to the above-mentioned problems could be the application of reconfigurable steganographic systems [1].

2. Reconfigurable steganographic system

The presented reconfigurable steganographic system has the following functionality:

- Secret sharing and recovering
- Checking validity of shares
- Embedding into steganographic containers
- Extracting from steganographic containers

Sharing and recovering of secret data is implemented basing on the Shamir threshold method of data division based on the principle of interpolation [2]. For the division of secret data $S$ using the threshold method $(M,N)$ it is necessary to choose polynomial $\phi(x)$ of $M-1$ with a free term of $S$ value and random coefficients of $a_1,...,a_{M-1}$. With the help of this polynomial, separate parts $S_i$ of secret $S$ can be calculated with the following formula.

$$S_i = S + a_1i + a_2i^2 + ... + a_{M-1}i^{M-1} \quad (1)$$

Each of the $S_i$ parts is then hidden in container files $\alpha$, $\{\alpha | \alpha = N\}$.

To recover the secret data $S$ participation of at least $M$ number of $S_i$ parts is necessary. These $M$ numbers are extracted from the relevant containers $\beta$, $\{|\beta| = M\}$, and through the application of Lagrange’s method of interpolation [3] the secret $S$ is then being recovered.

$$S = \sum_{i \in \beta} S_i \prod_{j \in \beta, j \neq i} \frac{j}{j-i} \quad (2)$$

Thus we have $N$ containers with embedded secret parts and by using $M$ containers we can recover the whole secret.

To check the validity of shares $p$ and $q$ numbers are randomly selected so that $p = 2 * q + 1$. A number $g$ is selected so that there is a congruence of $g^q \mod p = 1$. The following equations are calculated: $r_i = g_i^a \mod p, i = 1,2,...,t$. For the verification of the validity of this or that component of the secret data the congruence of the following equations are tested:
The user will be authenticated to the steganographic system when the set of actions performed by the user is exactly the same as in case of the registration. Only after a successful authentication a steganographic system will be executed.

To calculate the probability of an accidental authentication during normal operation with the graphical editor we limit the number of possible operations involved in construction of the steganographic authentication key by 60 and the maximum length of the steganographic key by 10. In this case all the possible combinations of the steganographic key will be calculated as follows:

\[
\binom{60}{10} = \binom{60 + 10 - 1}{7} = \binom{69}{7} = \frac{69!}{7!62!} \approx 10^9
\]

If we assume, that for performing each operation of steganographic key user needs 10 seconds, then the resulting value can be transferred in time complexity, which is \( \approx 342 \) years.

In fact, different authentication schemes or the second layer of authentication might be used. Nevertheless, use of alphanumeric passwords has certain drawbacks, e.g. passwords with high level of entropy are difficult to remember whereas passwords with low level of entropy are not secure. Biometric authentication is more secure but the weak point is that special hardware is needed. Nowadays schemes based on graphical passwords are alternative and developing trends in authentication systems.

The main idea of graphical passwords is that the majority of people remember better natural images and pictures rather than artificial words. For example, we can recognize familiar faces among thousands of strangers, and this phenomenon is used in the development of graphical authentication schemes. User can select a sequence of points if the image is big and complex and has high resolution (number of pixels).

In the proposed scheme the password consists of a sequence of mouse click points, that user selects in the image. The image itself is not a secret and bears no information for the scheme, it only helps the user to remember the click points positions.

To authenticate the user must click close to the points selected during the registration in the appropriate order. Since it is practically impossible for users to click several times on the same point, in the scheme we provide an error admission rate \( r \) in click locations (i.e. the disk with radius \( r = 10 \) or 15 pixels). This is implemented by discretization of click locations using three different square grids [5].

The distance between the gridlines of each grid (horizontal or vertical) is 6r. Each of the three grids shifted in a staggered order by 2r vertically and 2r horizontally:

\[
g^S (r_1 \mod p) = r_0 \ast (r_1)^i \ast \ast (r_i)^j \mod (p) \quad (3)
\]

Therefore, if the congruence of the equation (3) works, we can be sure that the tested component, has not been modified or generally replaced by other data, and hence can be used in the process of recovering the secret data [4].

Embedding into steganographic containers as well as extracting, is implemented in the steganographic system with the help of the known algorithms. As steganographic container can be considered any digital file, for which embedding and extracting algorithms have already been developed. In the reconfigurable steganographic system new steganographic methods can be added as addons or plugins.

The steganographic system with a dynamically reconfigurable structure increases security, integrity and availability of the secret information.

Existence of steganographic software on the computer system is suspicious therefore the application of steganography is secret by itself. Thus steganographic software should be hidden and not obviously present in the computer system.

Any security system should have authentication means, to be sure, that only authenticated users can access the secret data. Regular authentication mechanisms show the existence of secret information or system. That’s why regular authentication is not acceptable for steganographic system.

To ensure high secrecy and at the same time providing steganographic (hidden) authentication we propose a method based on the behavior (a set of actions) in an ordinary program, under which a steganographic system itself is hidden. In this paper, a graphic editor is considered as an ordinary program.

Let’s denote operations of graphical editor as 
\[
d_i (a_{i1}, a_{i2}, ..., a_{in})
\]

where \( a_j \) is the parameter \( j \) of operation \( i \) in graphic editor. We also define two main operations, \( d' \) as the first operation of the steganographic key and \( d^m \) as the final one. The secret steganographic authentication key to the behavioural authentication is the following sequence of operations:

\[
D=d', d_1 (a_{11}, a_{12}, ..., a_{1n}), d_2 (a_{21}, a_{22}, ..., a_{2n}), ..., d_k (a_{k1}, a_{k2}, ..., a_{kn}), d^m
\]

where \( k \) is the number of operations in the steganographic key and \( n_j \) is the number of parameters in the operation \( i \).

\[
(4)
\]
Fig. 1 Three grids map. G1, G2, and G3. Point T is in grid G1. Point R is in G2 and G3.

If there were only one discretization grid, the mouse click point might be close to the grid line and slight variations in the click points might result in an incorrect password. On the other hand, it is proved that in case of three staggered grids, the distance of any point in a two-dimensional picture from the grid lines doesn’t exceed r [5].

Because of the simultaneous use of multiple grids the selected points are "resistant" to the inevitable minor uncertainties in the point selection; therefore this method of discretization is called "stable discretization" or "stable quantization". Selected positions (click points) are applied to the grids map. The sequence of the selected points is the sequence of grids and grid squares, i.e. \( G_1, G_2, \) and \( G_3 \). Values are calculated for each mouse click, for example, the value of \( R \) is \( G_1(-4,-2)G_2(1,2)G_3(1,2) \). A negative value indicates that the circle crosses the relevant horizontal or vertical grid line. To ensure a secure storage of passwords in the system the sequence of grid squares is encrypted using cryptographic hash function.

One of the main attributes of the proposed scheme is that for graphical password creation can be used complex pictures of the real world as well as users can enter their own images. Natural images help users better remember complex passwords. Thus, in the "human context" (i.e. with the participation of users), conditional entropy of password depends on the underlying image.

In 2007 scientists from the University of Carleton, proved using ANOVA analysis tool that the image has a significant influence on the result of authentication [6]. In this sense "quality picture" is a picture on which the user can find a lot of parts (focal points) differing from the background and from each other, which may be potential points for the password. We also tried to determine the optimal size of these focal points by statistical experiment.

Two groups of people were involved in the experiment: students with computer skills and people without such. Such a selection is to provide an opportunity to determine the optimal focal point size for users with different skills.

In the first (registration) phase of the experiment, participants were asked to choose any complex image, select three points in this image and remember their location and selection order. In the second (authentication) phase participants should repeat these points 20 times.

As a result, during the experiments the error of the selected points (phase 2) was calculated in comparison with the original ones (points selected in the first phase). Based on the results of 838 qualitative efforts out of 1000, we determined the optimal value of the focal points. Fig. 2 presents the outcome experimental data (abscissa corresponds to the distance between the registered point and the authentication point, the ordinate shows the frequency of this distance).

The experiment revealed that for 97% of authentications, distances between the registered point and the authentication point lay within the range of 1 to 14 pixels, therefore, to reduce the number of authentication failures we choose \( r = 14 \).

To calculate the probability of accidental authentication, we limit the authentication image size by \( 1204 \times 768 \) pixels and the number of points selected as password by 6. In case of such limitations, the maximum number of the possible passwords for graphical and alphanumeric passwords are calculated as follows:

- for alphanumeric passwords with upper and lower case letters, special symbols and numbers maximum number of the possible passwords equals 966
- for graphical passwords the maximum number of the possible passwords is calculated as follows:

\[
\left( \frac{H \cdot W}{(2r)^2} \right) \left( \frac{k}{4r^2 + k - 1} \right) \approx 10^{18} \quad (6),
\]

where \( k \) is the number of points in the password, \( H \) and \( W \) are the height and width and \( r \) is the error admission rate.
In Fig. 3 the stability of alphanumeric and graphical passwords are compared which shows the dependence of the brute force time on the number of characters in a password.

4. Conclusion

The paper describes reconfigurable steganographic system which includes methods for secret sharing and recovering, checking validity of shares, embedding into steganographic containers extracting from steganographic containers. For the described system double layered hidden authentication mechanism has been proposed. Behavioral authentication based on the user’s behavior in graphical editor has been proposed as the first layer of authentication. A mechanism based on graphical passwords has been proposed for the second layer of authentication. The paper also points out the effectiveness of the proposed authentication mechanisms.

5. References:


