User Authorization in the Picture Password System with Application of Digital Watermarks

Alexey Shokarev
Yurga Institute of Technology
TPU
Yurga, Russia
shokarev av@mail.ru

Evgeny Kostyuchenko
Security Department
TUSUR
Tomsk, Russia
key@keva.tusur.ru

***Abstract*— The paper considers the method of user authorization in the graphical password system which is based on steganographical methods. The authors describes the generalized model of user authorization in secure systems with application of digital watermarks, the general model of the graphic password system, and lists the main requirements for digital watermarks to be used in the graphics systems of user authorization for protected information and telecommunication resources.**

Keywords—component; picture password, steganograph, watermark

I. Introduction

Users have certain difficulties with memorization of complex, pseudo – random passwords for a certain period of time. Most of them forget the password which is not used regularly. The situation when the user has several passwords for various systems is a common event today. The user may either mix the elements of different passwords or remember the password but forget which system it is for. [7].

The users generally cope with the problem of password memorization by reducing the complexity and the number of passwords, thus, increasing the risk of system cracking. The strong password must include at least 8 characters, preferably random, with upper and lower case characters, figures and special symbols. The users have problems with memorization of such passwords. In most cases users ignore the recommendations and use short, simple passwords which are relatively easy to discover. Practice shows that users often choose short passwords consisting of family or friends names, surnames, names of domestic animals, the word “password” is often used, too [7]. To avoid forgetting the password people often put them down or use the same password for several systems, sometimes with an only figure in the end.

II. Description of the Model of Picture Password Authentication

Due to the difficulty of password memorization and due to reducing the degree of system protection by the users, various institutes and universities all over the world are developing picture password systems aimed at releasing the users from learning complex passwords and increasing the degree of protection of various resources [1,6]. One of the disadvantages of the developed picture password systems is that most of them are based upon allocation of certain characters to the image chosen by the user for authentication. The system of picture passwords on the base of digital watermarks suggested below is free from this disadvantage due to introducing random characters generated by random bit pattern generator [5].

The suggested model of digital watermarks for user access differentiation to the protected resources applied in building the picture password system [10] is shown in Figure 1.

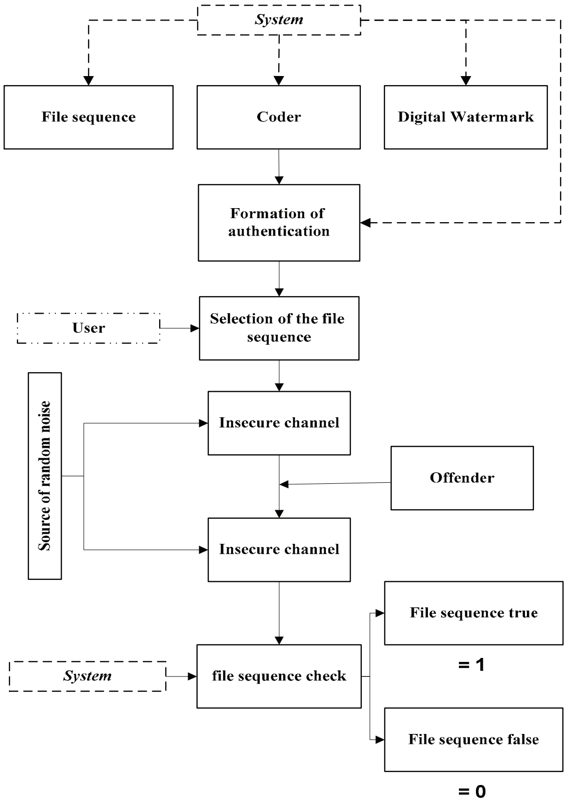

Figure 1 – The generalized model of authentication system

The system suggests the user choosing the succession of graphics files, and then the system impresses a digital watermark ***W*** on all the suggested graphics files. The mark, individual for every graphic object, is transformed in the coder for embedding into the authenticated message. The algorithm of formation of such watermark structure A is presented as:

$$A = F(I, W)$$

Where F is a function, depending on I – container (graphic file), W is the water mark.

Then, in the authenticated message originator the watermark A structure is build into the graphic container with the help of function Z, applying the confidential key K:

$$Z = \Psi(A, I, K)$$

Where Ψ is a function, depending on A – watermark structure, I is container (graphic file) and K – is the secret key.

After the user selects the sequence of graphical objects for his/her authentication the system channelizes it. In the communication channel the authenticated message Y is impacted by the penetrator as well as by random and intentional noise. As a result of this impact the examination device for the watermarks receives the modified message Y. By watermark detection algorithm the estimation W' of the watermark is formed:

$$W' = G(Y, W, K)$$

Where G – is a function with dependences on Y – modified message, W is the watermark, K a secret key.

User authenticity is determined according to this estimation. The possible answers may look as $W' = 1$ (message authenticity confirmed) or $W' = 0$ (message authenticity is not confirmed). Also, other messages are possible like $0,5 \leq W_j' \leq 1$ (j—th fragment is likely to be authentic) or $0 \leq W_j' < 0,5$ (j—th fragment is likely to be imposed or corrupted by the noises of message transfer). When forming the watermark estimation there may arise the underflow errors with the message receiver [2,10].

III. DESCRIPTION OF THE GENERAL MODEL OF THE PICTURE PASSWORD SYSTEM

In comparison to the cryptographic authentication systems the system of user authentication based on digital water marks has the following peculiarities:

- the authenticated message and the digital watermark imbedded into it are mutually dependent, which means that destruction of the first leads to the destruction of the second, and if the watermark retains its integrity the same happens to the received message;
- when receiving the corrupted fragment of the message the recipient may dismiss the given fragment without dismissing the whole message.

As opposed to the comparative methods the methods of authenticity control based on watermarks have significant advantages:

- high resistance to removing the authenticator of the authenticated message without destruction of the message itself;
- revealing the unauthorized reproduction of the authenticated messages;
- consistency with the sources of the messages having significant statistical dependences and memory, such as picture and acoustic signal.

The received picture password system is based on the application of steganographic methods [4] which increase the security of the whole authentication system in relation to the current picture password systems. The generalized model of user registration and authorization is shown in Figure 2 and Figure 3.

The suggested system has the following stages:

1. Registration of the user:

- Administrator of the system selects N graphical objects to be suggested to the user for authentication;
- The generator generates random sequences of characters including figures and small and capital Latin and Cyrillic letters;
- The steganographic subsystem completes embedding of the received sequences in the form of digital watermark with the secret key K;
- The user or the administrator introduces the name of the future user. Then the picture password system suggests N graphical objects selected by the administrator of the system with digital watermarks already imbedded into them to select a certain amount of them <N and to remember the sequence of their choice;
- The server end of the picture password system bases the new user and compares the extracted digital watermarks in the form of characters to his/her login.

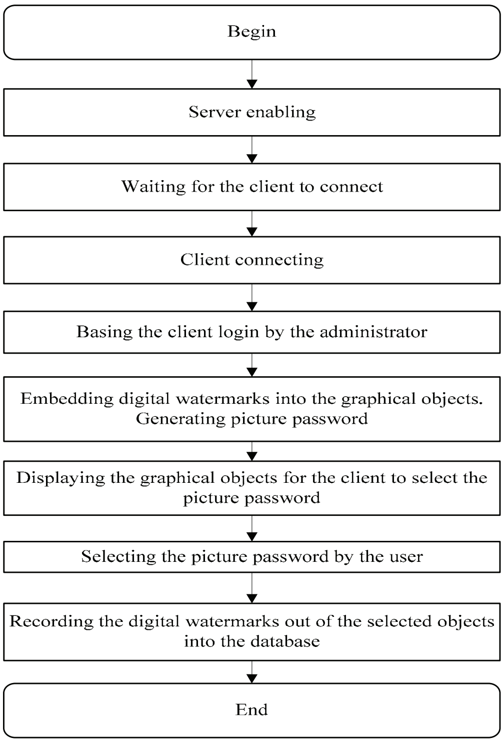
Begin
Server enabling
Waiting for the client to connect
Client connecting
Basing the client login by the administrator
Embedding digital watermarks into the graphical objects. Generating picture password
Displaying the graphical objects for the client to select the picture password
Selecting the picture password by the user
Recording the digital watermarks out of the selected objects into the database
End

Figure 2. Registration of a new user

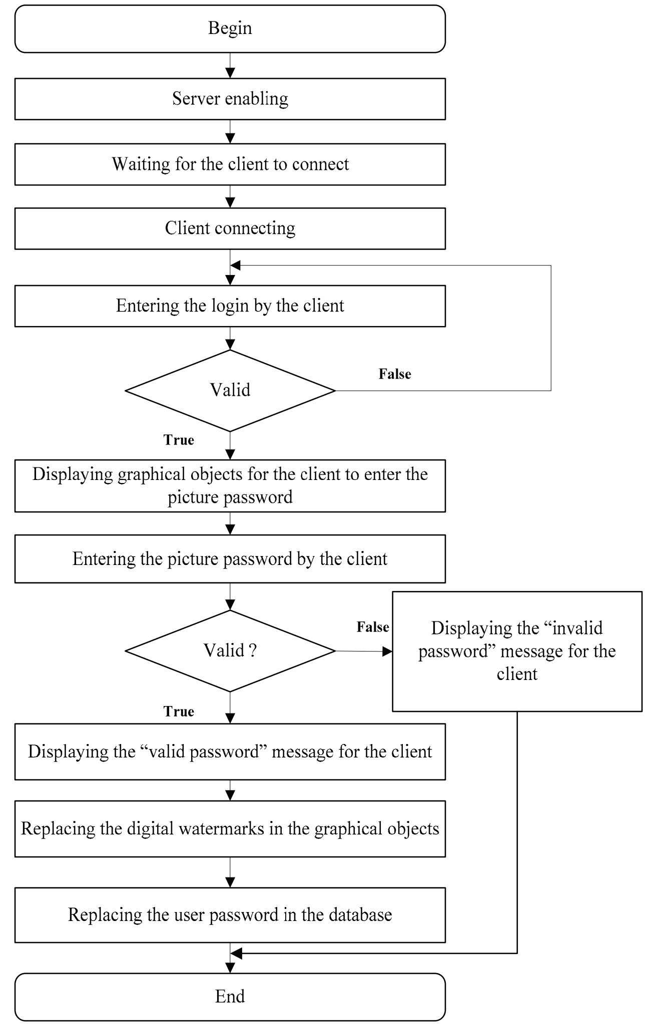
Begin
Server enabling
Waiting for the client to connect
Client connecting
Entering the login by the client
Valid
False
True
Displaying graphical objects for the client to enter the picture password
Entering the picture password by the client
Valid ?
False
Displaying the "invalid password" message for the client
True
Displaying the "valid password" message for the client
Replacing the digital watermarks in the graphical objects
Replacing the user password in the database
End

Figure 3. User identification/authentication in the picture password system

2. User authentication:

- To access the protected resource the client end of the picture password system suggests the user to enter his/her login and to select the same sequence of graphical objects offered by the system as it was done during the registration;
- In the server end the user login and the received digital watermarks are compared to the data in the database. If the digital watermark is the same as the registered sequence the user will enter the system, otherwise the system informs about faulty input;
- In case of successful completion the system generates new sequences of symbols and sends them to the client end to be further embedded into all present N graphic files. The new sequence used as the user password is put into the database on the server;
- When the client end of the system is called next time the graphical objects are arranged *in random order.*

The algorithm of the digital watermark embedding comprises three basic stages [3,4]:

- Digital watermark generation
- Digital watermark embedding in the coder
- Digital watermark detection in the detector.

Let us consider digital watermark generation.

Let ***W****, ***K****, ***I**** and ***B**** be the set of possible digital watermarks, keys, containers and hidden characters accordingly. Then/ generation of the digital watermark can be presented as follows:

$$F : I^* \times K^* \times B^* \rightarrow W^*, \quad W = F(I, K, B),$$

where ***I***, ***K***, ***B*** – represent the corresponding sets. Generally speaking function F can be arbitrary but in practice digital watermark robustness impose certain restrictions upon it. As, in most cases, $F(I,K,B) \approx F(I+\varepsilon,K,B)$ so the insignificantly changed container does not change the digital watermark. Function ***F*** is usually a composition one:

$$F = T \circ G \text{, where } G : K^* \times B^* \rightarrow C^* \text{ and}$$
$$T : C^* \times I^* \rightarrow W^*.$$

Operator T modifies the codewords C^*, which results in digital watermark W^*. This function may not be imposed the restriction of irreversibility as it is ensured by the appropriate choice ***G***. Function ***F*** must be selected in such a way that the empty container I_0, the filled container I_w and the insignificantly modified filled container I'_w would generate the same digital watermark:

$$T(C, I_0) = T(C, I_w) = T(C, I_w)$$

That means that it must be robust [9] and, accordingly, resistant to minor corruptions of the container.

The process of embedding the digital watermark ***W(i,j)*** into the initial image $I_0(i,j)$ is described as the superposition of two signals:

$$\varepsilon : I^* \times W^* \times L^* \rightarrow I_w^*,$$
$$I_w(i,j) = I_0(i,j) \oplus L(i,j) W(i,j) p(i,j).$$

Where ***L(i,j)*** is the mask of digital watermark embedding which takes into consideration the characteristics of the human visual system and serves for reducing the noticeability of the watermark.

$p(i,j)$ is the projection function depending upon the secret key ***K***. The aim of the given function is to spread the digital watermark through the graphic file.

The most important part of the steganographic system is the stego detector [8]. According to its type it can provide the solutions of various number languages about digital watermark presence or absence (in the case of soft—decision detector).

Let us consider a simpler case of “rigid” stego detector. Let us denote the operation of detecting through D. Then:

$$D : I_w^* \times K^* \to \{0,1\},$$

$$D(I_w, W) = D(I_w, F(I_w, K)) = \begin{cases} 1, & if\ W\ is \\ 0, & if\ W\ no \end{cases}$$

IV. Conclusion

From the user authentication models and picture password systems described above we can single out the basic requirements for the digital watermark systems applied for user authorization in the protected systems. The given systems must have the following properties:

- spoofing resistance, i.e. the impossibility for the penetrator who does not know the confidential key of the signature to form any message with the formally correct watermark;
- practical absence of non—detectable unauthorized reproduction of the authenticated message;
- when several messages with different watermarks are embedded into one container, the sequence of signatures must be traced and the signatures must not destroy each other;
- the impossibility of repudiation of the signed message (for the systems with confidential signature key and public verification key);
- the impossibility for the recipient to form the formally correct watermark of the message sender (for the systems with confidential signature key and public verification key);
- impossibility of deleting or destroying the watermark without destroying the message;
- watermark resistance to random and intentional noise which do not lead to destruction of the information content of the authorized message;
- formation and verification of the message watermark does not require the third trusted party;
- compatibility with the modern methods of transfer, storing, cryptographical security and noise resistance increase;
- the opportunity of authorized message processing with standard methods (stuffing, scaling, screening, compaction, etc.) without destroying the watermarks.

Safety of the suggested method of user authentication on the base of digital watermark will depend upon a number of factors:

- the more graphical objects the system suggests for the user to select, the harder is for the penetrator to carry out the exhaustive key testing;
- access to the system must be completed in accordance with the strict sequence of the graphical objects selected by the user as a password;
- the minimal succession for authentication must include at least three graphical objects;
- the graphical objects signed with digital watermarks and screened for authentication must be deposited only in the disk space of the user’s computer and contain only the user’s data for authentication in the system. This will allow avoiding cracking of the whole system;
- the user must not have full rights to use the protected resource;
- when digital watermark embedding unformatted methods are to be used;
- at every dialogue box launching the system must randomly change the graphical objects screened for authentication;
- after every successful user authentication the digital watermarks must be replaced in all graphical objects applied for user authentication (using one—time passwords);
- the system must use several embedding methods to be resistant to digital watermark cracking.

The suggested method of picture password has the following key features:

- for the first time digital watermarks are used for user identification/authentication in picture password systems.
- graphical objects are changed randomly, which makes the system invulnerable when glancing or using the keystroke registration programs and programs registering the coordinates of the mouse choosing the graphical objects.
- application of digital watermarks as one—time passwords make the system invulnerable for network packet capture.
- depositing the graphical objects in the user workplace does not allow the penetrator cracking the whole system.

Application of the suggested authentication method allows the user faster memorization of the passwords and increases the resistance of the picture password systems using the digital watermarks to being cracked by penetrators and also reduces the user authorization time in the systems. The described picture password system applies one—time passwords for authorization and, after the user successfully enters the system, automatically changes the digital watermarks in the graphical objects which surely makes capturing the transmitted sequence useless for authorization.

Acknowledgment

This work was supported by the Ministry of Educationand Science of the Russian Federation within federal targeted program Research and development in priority areas of scientific—technological complex of Russia for 2014 — 2020 (grant agreement 14.577.21.0153 on November 28, 2014, identifier RFMEFI57714X0153).

REFERENCES

[1] S.Brostoff,, M.A. Sasse “Are Passfaces more usable than passwords: A field trial investigation” People and Computers XIV - Usability or Else, Proceedings of HCI, 2000, P. 405-424.

[2] S. Craver “On public-key steganography in the presence of an active warden.” Proc. 2nd Intern Workshop on Inform. Hiding, 1998, LNCS, v.1525, 355-368.

[3] H. Farid “Detection Steganographic Message in Digital Images” Technical Report TR2001-412, 2001.

[4] F.A. Petitcolas, R.J. Anderson, M.G. Kuhn ”Information hiding – a survey” Proceeding of the IEEE, vol. 87, № 7, 1999, pp.1062–1078.

[5] A.V. Shokarev. ”Current Graphical Password Systems. Implementation Algorithms by Digital Watermarking” Applied Mechanics and Materials., 2013, Vol. 379. - p. 229-234

[6] L. Sobrado, J.C. Birget, ”Graphical passwords. ” The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol. 4, 2002.

[7] A.A. Afanasyev, L.T. Vedenyev, A.A. Vorontsov and others. ”Authentication. Theory and practice of secure access ensuring to information resources” Study guide for higher educational institutions. – M.: Goryachaya liniya – Telekom, 2009. 552 p.

[8] V.G. Gribunin, I.N. Okov, I.V. Turintsev ”Digital steganography” Moscow.: Solon-Press, 2009. 272 p.

[9] A.A. Shelupanov, A.V. Shokarev ”Theoretic-informational and complexity-theoretic approach for assessing the steganographic system resistance” SibSAU reporter “System integration and security”, Krasnoyarsk, 2006. Special edition. P. 121-123.

[10] . S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy and N. Memon “PassPoints: Design and longitudinal evaluation of a graphical password system.” Int. Journal of Human- Computer Studies 63, 2005, P102-127.