Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 3, March - 2015

A Secure Web Application Based Visual Cryptography and Secret Sharing

Ibrahim Levent Belenli[1] Turker Tuncer[2] Fahrettin Burak Demir[3] Engin Avci[4] Mustafa Ulas[5]
Firat University Department of Software Engineering, 23119 Elazig, TURKEY[1]
Firat University Department of Digital Forensic Engineering, 23119 Elazig, TURKEY[2]
Inonu University Department of Computer Engineering, 44000 Malatya, TURKEY[3]
Firat University Department of Software Engineering, 23119 Elazig, TURKEY[4]
Firat University Department of Software Engineering, 23119 Elazig, TURKEY[5]
ibrahim.belenli@inonu.edu.tr

***Abstract*— Nowadays, the transferred knowledge to reach the desired goal via the safety way begins to be more importance with the development of technology. The science of information security consists of some sub-branches such as steganography, cryptography and authentication. In this study, to avoid hacking and to provide information security is intended. In this study, the web-based user login system with using encryption-based visual secret sharing is prepared to increase in information security. Prepared system purposes authentication, previously such pixel-based authentication system has not been found in the web environment. Naor and Pinkas issued the article in 1997 is titled "Visual Authentication and Identification" which are discussed could be made of such a system.**

***Keywords*— Secret Sharing; Visual Cryptography; Image Processing; Information Security;**

I. INTRODUCTION

The methods such as cryptography or steganography are used to prevent undesired people's access to the data which is requested to be stored. Secret sharing techniques have also a special place among these techniques. The purpose of secret sharing methods is the sharing of data among n person. None of the n numbers data themselves does represent main data only if k number of pieces comes together the main data may be created. Thus, the data would not be under a single person's responsibility. The most well-known methods of secret sharing are Shamir, Blakley, Thien-Lin and Asmuth – Bloom ones. [1]. In the article written by Naor ve Pinkas [2] in 1997, it has been mentioned that secret share-based image encryption system can be used in online system and the application of this idea was realized then it was patented. The segment model of secret share-based image encryption technique has been used after 2005. In this study, the system which will be applied is pixel-based and in web applications, it is considered that it should be a system which prevents the case of theft of password. In 2th section of the study secret sharing methods, in 3th section Shamir's secret sharing method, in 4th section web-based application and in 5th section conclusions and recommendations will be discussed.

II. SECRET-SHARING METHODS

Nowadays, information security has become necessary because of the increasing internet speed and sharing all data via internet. Especially, if the information of institutions that should remain within themselves is captured by someone else, this may cause great difficulties. It has revealed the fact that transmitting information as pure information will cause major drawbacks. For this reason, in order to send data encryption steganography, secret sharing techniques can be used. Secret sharing method was introduced independently of one another by Shamir [3] ve Blakley [4] for the first time in 1979 [14]. Also, this method is called (k, n) threshold scheme. The main idea of the scheme is sharing confidential information among n person, regaining confidential information. By means of this technique which is also called Threshold Secret Sharing Technique, data security is isolated from the responsibility of a single person and it can be achieved in a more effective way [1].

Shamir has proposed a polynomial based method for performing (k, n) threshold scheme. The user creates a (k-1).order polynomial for (k, n) threshold scheme. Confidential data is the constant term of the polynomial, the polynomial coefficients are determined randomly by the user. As a user ID that is assigned the value of x corresponding to y values in the xy plane create share value to be sent. During the reconstruction phase with the (x, y) pairs of any of the k participants, previously hidden information is recovered by the use of Lagrange interpolation technique. Blakley suggested a geometric-based method. As it is known, the equation of a plane in three-dimensional plane is indicative of an infinite number of points. e intersection of two planes is a straight line so still represents an infinite number of point. Finally, the intersection of three planes can refer to a single point.(We accept that the plane is not parallel)[15]. In this case each of three people is given a different plane equation, when these k-dimensional three people come together, they can be provided to find one point. In case one or both of the parties come together, there will be an infinite number of points [5]. If we generalize this, Blakley started from confidential data being a point in a k-dimensional space. The number of n different Hyper-plane equation is pass on one point that is the information will be sent to

participants. The intersection of any k-grain hyper-plane gives confidential information in there.

The concept of sharing of privacy has been expanded to the field of vision by Naor and Shamir, and developed the encryption system that does not need a computer account only the human visual system (the eye) to decrypt [6]. To improve this scheme proposed by Naor and Shamir a variety of workspaces were formed. Thien and Lin proposed Shamir's secret sharing method in order to share secret images. [7]. Composed sharing images being in the form of noise may attract the attention of malevolent person and because this would jeopardize the security of the system, it has led to studies of hiding the image into another image with steganography and sharing later on [8].

In order to share confidential information there are also methods using properties of number theory. Asmuth-Bloom ve Mignotte, CRT (Chinese Remainder Theory) can be shown as examples of methods in this category. [1,9,10].

III. Shamir's (k,n) Secret Sharing Methods With Threshold

Shamir 's secret sharing method can be defined in a unique way with a polynomial of degree k-1 valueted differently on k point. Shamir 's secret sharing scheme is based on interpolation of Langran [2]. Given a set of points (xi, yi) (i = 0,1,2,3, ., k) based on interpolations Langrange name of Lk (x) is a polynomial function which using the following formula

$$f^k(x) = \sum_{i=0}^{k} y_i \prod_{j=0;i\neq j}^{k} \frac{x - x_i}{x_j - x_i}$$

Shamir realized in a limited area using polynomial interpolation as modular arithmetic instead of using real arithmetic.

Methods as Follows;

Step 1: to be s∈S a secret is selected.

Step 2: to be p>max(p,|S|) a Zp is selected

Step 3: to be a1, a2,.,ak-1∈Zp selecting k-1 coefficients independently and randomly is generated

f (0) = S a polynomial

f(x)=s+a1x+a2x2+.+ak-1xk-1 mod p (a0=s)

Step 4: For 1≤i≤n parts of secret is calculated as si=f(i) and components is distributed [11].

K in the formula indicate the number of receiver y values indicate the color values in the image parts. Both mode value used for folding and for composition [12].

The method described above may be performed using the visual secrets sharing. Each pixel is shown as a component of the two half-pixels. Pixel values is selected randomly and the pixel values is either 0 (black) or 1 (white). Secret parts are produced via this way and when these parts is subjected to an OR operation occurs secrets stands [16].

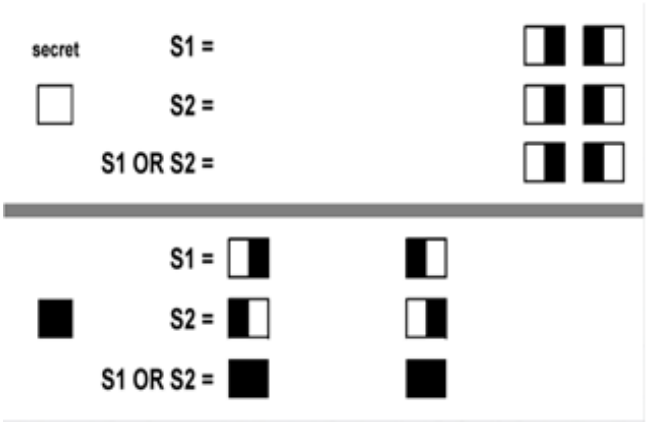

Figure 1: Visual secret sharing with the implementation of the OR operation

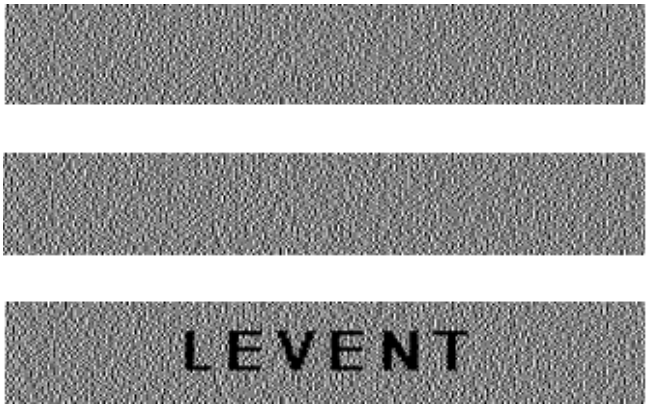

Figure 2: combination of the secret components obtain image password.

IV. Developed Web-Based Applications

As discussed above sections, today the biggest problem is to fight against spyware. Our internet passwords is likely to fall into the hands of others with trojans, key loggers, screen logger and other malicious software. For example, we want to transfer $ 10,000 using internet banking. Because of the fact that logging into the system made directly with the password, the passwords stolen through spyware software is common place. Security systems have developed models of screen keyboard in order to protect user passwords from key loggers but screen keyboard model can't maintain passwords against the screen logger. Systems for increasing the security of access to the system in the final stage uses one-time password. Owing to the fact that use one-time password imposes large costs for the company, mobile application to use one-time password is required.

In addition, continuous enter the password process is a waste of time and it adversely affects the usefulness of the existing system. The developed applications in Visual Studio 2012 Web Project is coded and the script language has been selected as the C # language. SQL was selected as the server database. Image encryption based on ımproved the secret sharing system the existing problems were to

be removed. The system is very easy to use the generated image is desired to provide security of the system. Record is made in the system and if the registration process is successful, the password is visualized. Visualization password is divided into 2 via using Shamir 's threshold secret sharing scheme(Optional number is 2, If desired image can be divided into more parts). Visualizing the first part of the password are in the database, 2 part is given to the user.

Figure 3: User registration screen

User registration screen is shown in Figure 3. In order to record in the system, extra information is not desired from the user. How to get register in other systems in the same way to this system. The only difference from other systems, user registration has been performed successfully, the system generates code shown in image for user as in Figure 4.

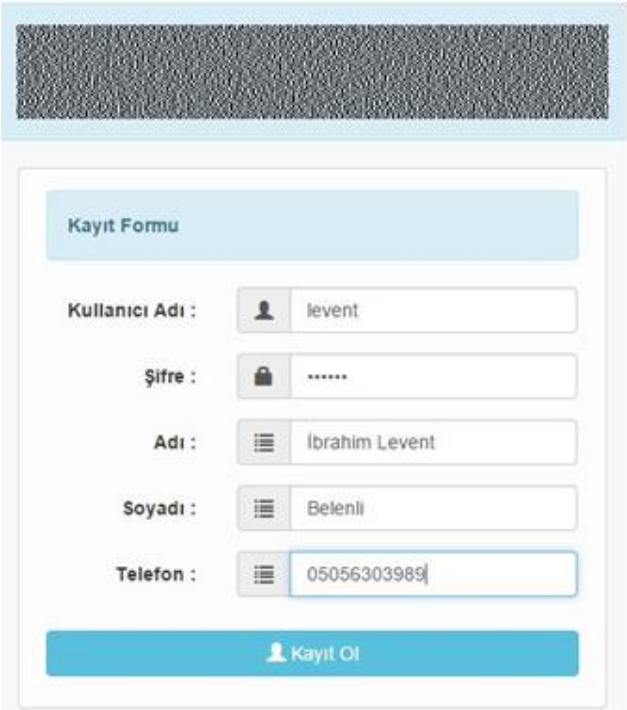

Figure 4: After successful registration process, defined imaginal password of the system for the user

After imaginal password is defined, user name and password are required as well as a visual one in order to log into the system. Login Screen is given in Figure 5.

Figure 5: Login screen

Operating steps of a user registration modules in the system are given below.

Step 1: It is checked whether the field has moved past the blank. If the blank left not to be filled, areas are issuing a warning to be filled.

Step 2: Information that the user is fully filled with a name that is associated with the key code is visualized.

Step 3: Visualization password is divided into 2 or n via Shamir's threshold secret sharing method.

Step 4: Formed part of the first secret key associated with the user name is saved in the SQL database. The other part is returned to the user.

Registration is performed as above and then user password is saved. As for the user to login, enter the user name and password, then upload the picture. System controls user name and password in the first place, ıf database user name and password is correct picture in the database and the picture of user superpose and then is obtained visual password. After obtaining the password text portion of the visual password is obtained by cleaning up noise operation. The password is compared with the user password to obtain accuracy. If passwords to match each one, entrance of the system is available. If ıt is not, the request is denied for entry. For example, get password "12345678". Visualization of password and the secret parts is shown in fıgure 6.

(a) (b) (c)

Figure 6: (a) visualizations of password (b) the first secret part (c) second secret part

Correlation coefficient gives the relationship between pictures and formula is as follows

$$r = \frac{\sum x_i y_i}{\sqrt{\sum x_i^2 \sum y_i^2}} = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

Correlation coefficients for our understanding of the relationship between the photos, we should look to Table 1 [13].

R	Relation
0-0,25	Very weak
0,25-0,50	Weak
0,50-0,70	Medium
0,70-0,90	High
0,90-1,00	Very high

Table 1: Interpretation of Pearson's Correlation Coefficient

V. Conclusion And Recommendations

In this study, Shamir 's threshold secret sharing method was carried out using a reliable web application. The main purpose of this application is to generate a new security tool as an alternative tool such as electronic signatures and to improve availability of the web-based applications . Many Internet-based systems request the form of password which consist of at least 8 characters and uppercase letters, lowercase letters, numbers and punctuation marks. Passwords generated using this method are stronger than a simple password created with only numbers or only letters but it is very difficult to provide persistence in mind. ASCII of characters consider an 8-digit password. In order to create a password that has a combination 264 units in 2568.

When we consider image encryption system in secrets of share-based to generate 100x100 visual password need for 210000 combinations. When we use this developed application both passwords will become more difficult to break and simple password can be used for catchy. When Shamir's threshold secret sharing scheme based chaotic systems combined with steganography is likely to be stronger in the future for creation of visual password.

Acknowledgements

The authors gratefully acknowledge funding of this

work by the TUBITAK (The Scientific and Technological Research Council of Turkey) (Project No: 2130120)

References

[1] Demir M.,Ulutaş M.,Odabaş E.,Asmuth Bloom Sır Paylaşımı Tekniğinin Hızlandırılması İçin Koşut Programlama,Elektrik-Elektronik ve Bilgisayar Sempozyumu 2011,Elazığ,Turkey,2011.

[2] Moni Naor and Benny Pinkas. Visual authentication and identication.In Lecture Notes in Computer Science, pages 322-336. Springer-Verlag,1997.

[3] A.H Uslu, R., Elektronik Bir Hücresel Yapay Sinir Ağı Gerçeklemesi Olan ACE16K Üzerinde Görüntü Bölütleme, Yüksek Lisans Tezi, İ.T.Ü., Fen Bilimleri Enstitüsü, İstanbul, 2007.

[4] Tang, J., A Color Image Segmentation Algorithm Based on Region Growing, Nisan 2010, 2nd International Conference on Computer Engineering and Technology (ICCET), Xi'an, China, Bildiriler Kitabı: 634 -637.

[5] Bischof, R., A. and Bischof, L., Seeded Region Growing, Pattern Analysis and Machine Intelligence, 16, 6 (1994) 641-647.

[6] Revol, C. and Jourlin, M., A new minimum variance region growing algorithm for image segmentation, Pattern Recognition Letters, 18, 3(1997) 249-258.

[7] Wan, S. and Higgins, W., E., Symmetric region growing, Image Processing, 12, 9 (2003) 1007-1015.

[8] Zhi, L. and Jie, Y., Interactive video object segmentation:fast seeded region merging approach, Electronics Letters, 40, 5 (2004) 1-2.

[9] Plataniotis, K., N. and Venetsanopoulos, A., N., Color Image Processing and Applications, First Edition, Springer, 2000, Almanya].

[10] Shih, F.,Y. and Cheng, S., Automatic Seeded Region Growing for Color Image Segmentation, Image and Vision Computing, 23 (2005) 877–886.

[11] http://htsencar.etu.edu.tr/Bahar10/bil553/ders10.pdf (28.05.2013 tarihinde bakıldı).

[12] Mesut A. Ş.,Mesut A.,Sakallı M.T., Görüntü Steganografide Gizlilik Paylaşım Şemalarının Kullanılması ve Güvenliğe Etkileri, Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, Ankara, 2010.

[13] http://www.doguc.com/H3.htm

[14] Chen, C.-C., Fu, W.-Y, “A Geometry Based Secret Image Sharing Approach”, Journal of Information Science and Engineering, Vol 24, No.5, pp. 1567-1577, 2008.

[15] Jasmin Oz and Assaf Naor,” Reed Solomon Encoder/Decoder on the StarCore™ SC140/SC1400 Cores, With Extended Examples”, Freescale Semiconductor Inc.

[16] C.C. Thien and J.C. Lin, “Secret image sharing,” Comput. Graph. 26, 765–770, 2002.