Access Control Based on Pixel Value Extraction

N.K.PREMA,
Associate Professor & Head/CSE,
Annai Teresa College of Engineering, Thirunavalur, India
premasenthi@gmail.com

Abstract: - This paper is to introduce a new access control method based on image file's pixel value. The method is aim to be invincible from key-logger software. Key-logger is a spy-ware that resides in a workstation to log every key-stroke, and the key-stroke logs are accessible through remote location. Key-logger is able to get every single character typed-in in plain-text. Passwords that should be confidential are readable easily when the key-stroke logs being retrieve by hacker. Pixel Value user access control method is not involving password key-in on a workstation. The password has been stored in server and it is a pixel value generated from extracted image file through image compression algorithm, in example Discrete Cosine Transform (DCT). Image compression algorithm is a series of mathematical functions that calculate color composition on single image file and usually used to authenticate watermarking on image. The algorithm produces pixel value that used as password to authenticate a user access. It is secretly kept on database and even users have no idea what is the password. User only need to upload their security image, so called passpict in order to log-in. Pixel Value user access control can be suitable to implement on web-based application log-in such as web-mail, social network, online portal, and banking portal.

Key-Words: - Pixel Value, Image Compression Algorithm, Authentication, Log-in, Passpict.

I. INTRODUCTION

Pixel value access control is a method to provide a new secure guard mechanism for access control on online or any web based system. It is a way to avoid end user to key-in their password being capture by key-logger software. With a pixel value access control guarded system, an image will be used to authenticate their identity; it is so call *Passpict* rather than password as authentication [1].

The end-user required to upload their known image in order to log in to an online system. When the server receives the *passpict*, the system will extract pixel value from the picture and used its value as authentication value for respective user-name. The way to extract pixel value from an image is using Image compression techniques. There are various imaging compression algorithms and each compression techniques produce an output in quantitative value or known as pixels value. The pixels value will be used to authenticate a user-name. The end users are authenticated and authorized to access their resource on the network without entering passwords. Key-logger software got no keystroke capture, and the end-user account is safe. Through this paper, image compression, pixel value concept, DCT and its process are briefly explained in section 1. Section 2 of this paper listed some related image authentication or graphical password design and implementation. On section 3, proposed method, discuss on current implementation problem and proposed solution design. Conclusion and significant of this method will discuss on section 4.

1.1 Image Compression

Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. This is because lossy compression methods, especially when used at low bit rates introduce compression artifacts [2]. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that produces imperceptible differences may be called visually lossless [3].

1.2 Pixel Value

A pixel is generally thought of as the smallest single component of a digital image. However, the definition is highly context-sensitive. For example, there can be "printed pixels" in a page, or pixels carried by electronic signals, or represented by digital values, or pixels on a display device, or pixels in a digital camera (photo sensor elements) [4]. This list is not exhaustive, and depending on context, there are several terms that are synonymous in particular contexts, such as pel, sample, byte, bit, dot, spot, etc. The term "pixels" can be used in the abstract, or as a unit of measure, in particular when using pixels as a measure of resolution, such as: 2400 pixels per inch, 640 pixels per line, or spaced 10 pixels a part [5]. The measures dots per inch (dpi) and pixels per inch (ppi) are sometimes used interchangeably, but have distinct meanings, especially for printer devices, where dpi is a measure of the printer's density of dot (e.g. ink droplet) placement [6]. For example, a high-quality photographic image may be printed with 600 ppi on a 1200 dpi inkjet printer. Even higher dpi numbers, such as the 4800 dpi quoted by printer manufacturers since 2002, do not mean much in terms of achievable resolution. The more pixels used to represent an image, the closer the result can resemble the original.

The number of pixels in an image is sometimes called the resolution, though resolution has a more specific definition. Pixel counts can be expressed as a single number, as in a "three-mega pixel" digital camera, which has a nominal three million pixels, or as a pair of numbers, as in a "640 by 480 display", which has 640 pixels from side to side and 480 from top to bottom (as in a VGA display), and therefore has a total number of 640 × 480 = 307,200 pixels or 0.3 mega pixels. The pixels, or color samples, that form a digitized image (such as a JPEG file used on a web page) may or may not be in one-to-one correspondence with screen pixels, depending on how a computer displays an image [7]. In computing, an image composed of pixels is known as a *bitmapped image* or a *raster image*. The word *raster* originates from television scanning patterns, and has been widely used to describe similar halftone printing and storage techniques [8]. Each digital image files stored inside a computer has a pixel value which describes how bright that pixel is, and what color it should be. The most common pixel format is the byte image, where this number is stored as an 8-bit integer giving a range of possible values from 0 to 255. Typically zero is taken to be black, and 255 are taken to be white. During extraction through certain algorithm, the image files are dividing into grids; it can be 8 by 8 grid or 16 by 16 grids. Each grid is being calculated its pixel value with compression algorithm [9]. Then, all grids' pixel value will be transform into a single value with compression algorithm once again. This is how pixel value is being produce and acquire from an image. In this authentication method, pixel value will be used as authentication key for a user-name.

1.3 Discrete Cosine Transformation (DCT)

A **discrete cosine transform** (**DCT**) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations [10]. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer functions are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common [11].The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT", its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transforms (DST), which is equivalent to a DFT of real and *odd* functions, and the modified discrete cosine transforms (MDCT), which is based on a DCT of *overlapping* data.

1.4 Access Control

Access control refers to exerting control over who can interact with a resource. Often but not always, this involves an authority, who does the controlling [12]. The resource can be a given building, group of buildings, or computer-based information system. But it can also refer to a restroom stall where access is controlled by using a coin to open the door. Access control is, in reality, an everyday phenomenon. A lock on a car door is essentially a form of access control. A PIN on an ATM system at a bank is another means of access control [13]. The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment. *Item control or electronic key management* is an area within (and possibly integrated with) an access control system which concerns the managing of possession and location of small assets or physical (mechanical) keys [14].

1.4.1 Access Control Model

Access control models are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC is non-discretionary.

Attribute-based access control

In attribute-based access control (ABAC), access is granted not based on the rights of the subject associated with a user after authentication, but based on attributes of the user [15]. The user has to prove so called claims about his attributes to the access control engine. An attribute-based access control policy specifies which claims need to be satisfied in order to grant access to an object. For instance the claim could be "older than 18". Any user that can prove this claim is granted access. Users can be anonymous as authentication and identification are not strictly required [16]. One does however require means for proving claims anonymously. This can for instance be achieved using anonymous credentials or XACML (extensible access control markup language) [17].

Discretionary access control

Discretionary access control (DAC) is a policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have.

Two important concepts in DAC are [18]

- File and data ownership: Every object in the system has an *owner*. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
- Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.

- Access controls may be discretionary in ACL-based or capability-based access control systems [19]. (In capability-based systems, there is usually no explicit concept of 'owner', but the creator of an object has a similar degree of control over its access policy.)

Mandatory access control

Mandatory access control refers to allowing access to a resource if and only if rules exist that allows a given user to access the resource. It is difficult to manage but its use is usually justified when used to protect highly sensitive information [20]. Examples include certain government and military information. Management is often simplified (over what can be required) if the information can be protected using hierarchical access control, or by implementing sensitivity labels. What makes the method "mandatory" is the use of either rules or sensitivity labels [21].

- Sensitivity labels: In such a system subjects and objects must have labels assigned to them. A subject's sensitivity label specifies its level of trust. An object's sensitivity label specifies the level of trust required for access. In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.
- Data import and export: Controlling the import of information from other systems and export to other systems (including printers) is a critical function of these systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times.

Two methods are commonly used for applying mandatory access control:

- Rule-based (or label-based) access control: This type of control further defines specific conditions for access to a requested object. A Mandatory Access Control system implements a simple form of rule-based access control to determine whether access should be granted or denied by matching [23]:
  - An object's sensitivity label
  - A subject's sensitivity label
- Lattice-based access control: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.
-

Few systems implement MAC; XTS-400 and SELinux are examples of systems that do. The computer system at the company in the film *Tron* is an example from the prior century [24].

Role-based access control

Role-based access control (RBAC) is an access policy determined by the system, not the owner. RBAC is used in commercial applications and also in military systems, where multi-level security requirements may also exist. RBAC differs from DAC in that DAC allows users to control access to their resources, while in RBAC, access is controlled at the system level, outside of the user's control [25]. Although RBAC is non-discretionary, it can be distinguished from MAC primarily in the way permissions are handled [26]. MAC controls read and write permissions based on a user's clearance level and additional labels. RBAC controls collections of permissions that may include complex operations such as an e-commerce transaction, or may be as simple as read or write. A role in RBAC can be viewed as a set of permissions.

Three primary rules are defined for RBAC [27]:

1. Role assignment: A subject can execute a transaction only if the subject has selected or been assigned a role.
2. Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
3. Transaction authorization: A subject can execute a transaction only if the transaction is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.

Additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles. Most IT vendors offer RBAC in one or more products.

II. RELATED WORKS

In the United State of America, a lot of image based access control patents publication has been issued such as U.S. Patent No. 5,559,961 by Blonder, U.S. Patent Application Publication No. 2003/0191947 to Stubblefield, and U.S. Patent Application Publication No. 2004/0230843 to Jansen [29]. Based on these patents image based access control is applied for double layer protection for current log-in guard system. (User-name and password). When a user's user-name and password has been authenticate, user need to choose a image from the server library in order to proceed to their account. The image set has been provided by server and users need to choose from library collection. A single image can be used by multiple users by its default design. This design is known as graphical password. Graphical password for access control was implemented by MAYBANK. It has similarity with design that patent in U.S.A. MAYBANK, a Malaysians banking and financial institution, with their Online Banking service called Maybank2u.com [28], the client needs to select an image icon with their challenge phrase under that image that they selected. Now the user will save additional information to the Maybank2u.com server. This image with its challenge phrase will appear each and every time before a user specifies their password for log-in. The reason of this feature added, is to ensure that the bank knows something that the user know.

Image Compression Techniques has been widely used for image authentication to determine watermarking on a single digital image file [30]. Most picked compressions techniques are Discrete Cosine Transform and Wavelet Transform. Digital Watermarking purpose was for protecting digital imaging copyright and originality. In watermarking authentication, the picture will be extract into pixel value to find hiding pattern on image. Based on acquired pixel value, the brightness and darkness of each grid will determine watermarking pattern on image. Many techniques has been developed and applied for watermarking authentication purpose [31].

III. PROPOSE METHOD

Based on current implementation, the image that used to authenticate a user has been provided and it is common image libraries such as cartoon dinosaurs, dogs, and cars. In other words, the image libraries are viewable and exposed to everyone. With high intention of breaking into a user account, the security parameter can be by-pass by traditionally choose each available image on library properly. After a series of worth trying, hackers are successfully breaking into an account.

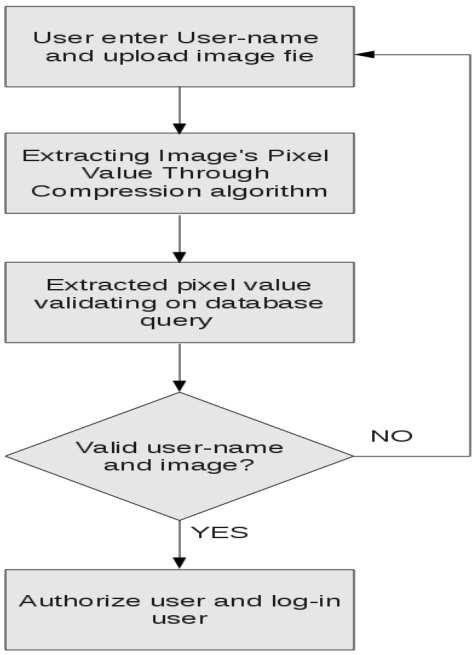

Figure 1. Log-in process for Pixel Value User Access Control

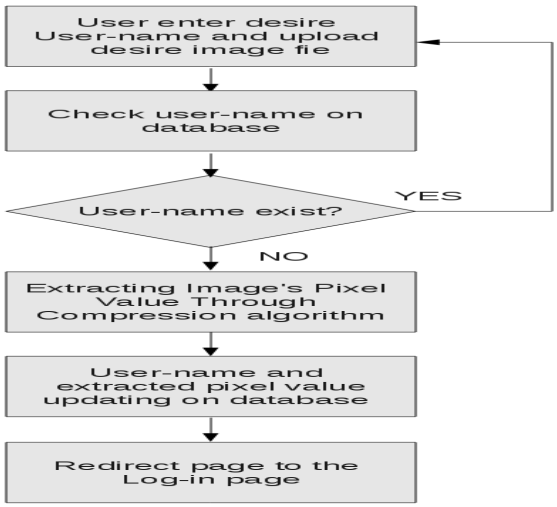

Figure 2. User enrollment process for pixel value user authentication

Theoretically, image brute-force tools can bypass this authentication system. Image brute-force tools attempt to find the correct image by scanning each image grid. For traditional log-in page, users require to key-in user-name and password. A hidden Key-logger will capture the actual user-name and password on an end-user workstation. The confidentiality of a password easily leaked not just through key-logger software, password can be easily obtained through simple spying techniques, shoulder suffer, as a person with malicious intent simply look the log-in or through private conversation eavesdropping. This proposed method is involving image as key-pass for a log-in system. Based on user-name - password concept and graphical password concept, pixel value user access control is combination of both concepts. With pixel value user access control method, users just need to enter user-name and upload their security image to the log-in page. The security image is just known by the user secretly, so called as *passpict,* and not keep on server. Efficiency of ECC is depends upon factors such as computational overheads, key size, bandwidth, ECC provides higher-strength per- bit which include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, smaller certificates and cluster using the density based, Sub-space, Evidence Accumulation Clustering

Server then, extract the uploaded image to get its' pixel value that will be used to authenticate a user. The pixel value is bringing to query for next authentication process. User-name and pixel value are being validate from user database. The user will grant for access if the user-name and pixel value is successfully passing the validating process. The user account details are storing in a database that containing user-name and pixel value. In order to enable or activate a user-name on log-in, users have to register their user-name and image file. This process require user to key in their user-name and upload their *passpict* as prerequisite for system. Other details such as full name will be just for system records. System itself will find user-name record for any existing user-name. If the user-name has been registered and existed on database, user need to chose another user-name and refill on enrollment page. For a newly register 'user-name, system will extract the uploaded image file to acquire its' pixel value through image compression algorithm. User-name, pixel value, and other records are being inserted into database. Enrolled user-name and image's pixel value are ready to being used on log-in page. Through pixel value user authentication method, user themselves have no information or idea what is the plain-text of their password since it is keep in their *passpict* file [32]. It is end user responsibility to keep the *passpict* safely from being use for identity theft. User may use a usual image file as *passpict* such as social network site profile picture, company logo, and image on personal blog, and any image file stored in USB drive, but no one should know it is a *passpict* file. User may keep their *passpict* on any digital space locally or online as long as it is reachable when it is needed.

IV. CONCLUSION

User access control based on pixel value is a hybrid log-in method from user-name – password concept and graphical password concept. Unlike current implementation, where user needs to pick a image from listed image libraries, this method will give user flexibility to use their own meaningful security image as their authentication parameters or *passpict.* Plus, it is easy to remember their own meaningful image rather than they need to choose image that meaningless to them. Hackers have no idea what image that user being use as *passpict* when it is securely kept by user. As traditional passwords, where user needs to renew their password periodically, *passpict* might be change by user as *Facebook* profile picture. This authentication method brings a lot of benefits which is:

- When a key pass transfer across the network without using conventional text format make cracking tools and method are unable to define the password.
- Key logger is unable to capture typing text when there is no password key in involving.
- Using image identification, much more easily to memorize than word phrase. Forgotten password issue will be reduce
- Upload module are replacing password text box will protect login page from brute force attack or dictionary attack.

REFERENCES

[1] R. R. Coifman and M. V. Wickerhauser, “Entropy-based algorithms for best basis selection,” *IEEE Trans. Inform. Theory*, vol. 38, pp. 713–718, Mar. 1992.
[2] A. Said and W. A. Pearlman, “A new fast and efficient image codec based on set partioning in hierarchical trees,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 6, pp. 243–250, 1996.
[3] J. M. Shapiro, “Embedded image coding using zerotrees of wavelet coefficients,”*IEEE Trans. Signal Processing*, vol. 41, pp. 3445–3462, Dec.1993.
[4] P. Sriram and M.W. Marcellin, “Image coding using wavelet transforms and entropy-constrained trellis quantization,” *IEEE Trans. Image Processing*,vol. 4, pp. 725–733, 1995.
[5] K. Ramchandran and M. Vetterli, “Best wavelet packet bases in a ratedistortion sense,” *IEEE Trans. Image Processing*, vol. 2, pp. 160–175, Apr. 1993.
[6] Y. Shoham and A. Gersho, “Efficient bit allocation for an arbitrary set of quantizers,” *IEEE Trans. Acoust., Speech, Signal Processing*, vol. 36, pp. 1445–1453, Sept. 1988.
[7] Z. Xiong, K. Ramchandran, and M. T. Orchard, “Wavelet packets coding using space-frequency quantization,” *IEEE Trans. Image Processing*, vol. 7, pp. 892–898, June 1998.

[8] G. J. Sullivan, "Efficient scalar quantization of exponential and Laplacian random variables," *IEEE Trans. Inform. Theory*, vol. 42, no. 5, pp. 1365–1374, Sept. 1996.
[9] M. Nelson and J.-L. Gailly, *The Data Compression Book*. New York: M&T, 1996.
[10] L. Cooper and M. W. Cooper, *Introduction to Dynamic Programming*. New York: Pergamon, 1988.
[11] T. Cover and J. Thomas, *Elements of Information Theory*, New York: Wiley, 1991.
[12] O. Rioul and P. Duhamel, "Fast algorithms for discrete and continuous wavelet transforms," *IEEE Trans. Inform. Theory*, vol. 38, pp. 569–586, Mar. 1992.
[13] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," *J. Fourier Anal. Applicat.*, to be published.
[14] R. E. Van Dyck and T. G. Marshall, "Ladder realizations of fast subband/ VQ coders with diamond support for color images," *IEEE Int. Symp. Circuits Syst.*, pp. I-670–I-677, 1993.
[15] A. A. C. Kalker and I. A. Shah, "Ladder structures for multidimensional linear phase perfect reconstruction filter banks and wavelets," in *Proc. Visual Communication Image Processing '92*, 1992, pp. 12–20.
[16] T. G. Marshall, "U-L block-triangular matrix and ladder realizations of subband coders," in *Proc. ICASSP 93*, 1993, pp. 177–180.
[17] E. Fossgaard, "Fast computational algorithms for the discrete wavelet transform," M.S. thesis, Dept. Math. Statist., Univ. Tromsø, Norway, Nov. 1997.
[18] K. A. Birney and T. R. Fischer, "On the modeling of DCT and subband image data for compression," *IEEE Trans. Image Processing*, vol. 4, pp. 186–193, Feb. 1995.
[19] G. M. Davis, "A wavelet-based analysis of fractal image compression," *IEEE Trans. Image Processing*, vol. 7, pp. 141–1545, Feb. 1998.
[20] A. S. Lewis and G. Knowles, "Image compression using the 2-D wavelet transform," *IEEE Trans. Image Processing*, vol. 1, pp. 244–250, Feb. 1992.
[21] N. M. Rajpoot, F. G. Meyer, R. G. Wilson, and R. R. Coifman, "On zerotree quantization for embbeded wavelet packet image coding," in *Proc. Int. Conf. Image Processing*, 1999.
[22] J. B. Buckheit and D. L. Donoho, "Wavelab and reproducible research," in *Wavelets and Statistics*, A. Antoniadis and G. Oppenheim, Eds. Berlin, Germany: Springer-Verlag, 1995, pp. 55–82.
[23] F. G. Meyer and R. R. Coifman, "Brushlets: A tool for directional image analysis and image compression," *Appl. Comput. Harmon. Anal.*, pp. 147–187, 1997.
[24] S. S. Chen, "Basis pursuit," Ph.D. dissertation, Dept. Statist., Stanford Univ., Stanford, CA, Nov. 1995.
[25] S. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionaries," *IEEE Trans. Signal Processing*, vol. 41, pp. 3397–3415, Dec. 1993.
[26] F. G. Meyer, A. Z. Averbuch, J.-O. Strömberg, and R. R. Coifman, "Multi-layered image representation: Application to image compression," in *Proc. IEEE Int. Conf. Image Processing*, 1998.
[27] United States Patent Application Publication. (2012). Graphical Image Authentication And Security System (Publication No. US 2012/0023574 A1). Portland, Orlando.
[28] Malayan Banking Berhad press release (2011). Maybank2u.com introduce additional security features. Retrieved July 5, 2011 from http://www.maybank.com.my/corporate-profile/corporate-news/maybank2ucom-introduces-additional-security-features
[29] Mona F.M. Mursi, Ghazy M.R. Assassa, Hatim A. Aboalsamh, & Khaled Alghathbar. (2009). A DCT - Based Secure JPEG Image Authentication Scheme. World Academy Of Science, Engineering and Technology, 682-687.
[30] Sumo Brain Solution. (2012). Graphical Image Authentication and Security System. Retrieved on 15 February 2012, from http://www.freepatentsonline.com/y2012/0023574.html
[31] R.Fisher,S.Perkins,A.Walker and E.Wolfart.(2003).Pixel Value, Retrieved on 21 December 2011, from http://homepages.inf.ed.ac.uk/rbf/HIPR2/value.htm
[32] Graves, Kimberly, (2010) CEH Certified Ethical Hacker Study Guide, John Wiley & Sons, Incorporated.