Enhanced Authetication Scheme Using Image Fuzion and Multishared Cryptography

Mr.Vijay B Gadicha1st
Department of Computer Science & Engineering
P.R.Patil College of Engineering & Technology
Amravati University, Amravati
V_gadicha@rediffmail.com

Dr. A.S.Alvi2nd
H.O.D, Department of Information Technology
P.R.M.I.T. & R, Badnera
Amravati University, Amravati

Abstract: The secret sharing schemes in conventional visual cryptography are characterized by encoding one shared secret into a set of random transparencies which reveal the secret to the human visual system when they are superimposed. The ordinary concept of secret sharing is sharing the secret key, and secret sharing schemes are also wildly used for secret transmission nowadays. But most secret sharing schemes are based on cryptography [3–11] such that the encryption and decryption processes need high computation costs. Visual cryptography, a kind of secret sharing schemes, differs from traditional secret sharing in terms of the efficient decryption process. This ultimately brings the downfall of the scheme. Therefore, we need a Password Generator Scheme which will restrict the Intruders to crack the password or we should design such a scheme which will cause sufficient delay in cracking of a password so that the Generator of the password changes the previous password.

Keywords- Component; Visual Cryptography ,Image Fusion

I. Introduction

1.1 Visual Cryptography

Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images(either binary or color) and number of secret images(either single or multiple) encrypted by the scheme.

Visual cryptography is introduced by first in 1994 Noar and Shamir [1]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. This paper provides overview of various visual cryptography schemes. Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. To meet the demand of today's multimedia information gray and color image format should be encoded by the schemes. Other performance measures such as contrast, accuracy, security and computational complexity that affect the efficiency of visual cryptography are also discussed in this paper.

1.2 Black and White Visual Cryptography Schemes

A) Sharing Single Secret

Naor and Shamir's[1] proposed encoding scheme to share a binary image into two shares Share1 and Share2 . If pixel is white one of the above two rows of Table 1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table1is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed.

B) Sharing Multiple Secrets

The visual cryptography schemes to share two secret images in two shares. They hidden two secret binary images into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by A⊗ B, and the second secret can be obtained by first rotating A ϴ anti-clockwise. They designed the rotation angle ϴ to be 90◦. However, it is easy to obtain that ϴ can be 180◦ or 270◦. To overcome the angle restriction of Wu and Chen's scheme [2], Hsu et al. [3] proposed a scheme to hide two secret images in two rectangular share images with arbitrary rotating angles. Wu and Chang [4] also refined the idea of Wu and Chen [2] by encoding shares to be circles so that the restrictions to the rotating angles (ϴ = 90◦, 180◦ or 270◦) can be removed.

1.3 Objectives

Current research work is dedicated to achieve some of the following objectives.

1. To impart & enhance the confidentiality of the secret information or data.
2. To device a user authentication system based on strong password, which can be obtained by using image fusion & visual cryptography.

3. To ensure the data integrity & availability by providing access to authentic users only To design a scheme which will overcome from all the threats created by various human generated or automated systems for the user authentication.
4. To realize a mechanism which will cause sufficient delay for an intruder to crack the valid user authentication (password)?
5. To realize a mechanism which will cause sufficient delay for an intruder to crack the valid user authentication (password)?

II. Review of Literature

Password-based authentication is the protocol that two entities share a password in advance and use the password as the basic of authentication. Existing password authentication scheme can be categorized into two types: weak password authentication schemes and strong-password authentication schemes. In general, strong-password authentication protocols have the advantages over the weak password authentication schemes in that their computational overhead are lighter, designs are simpler, and implementation are easier, and therefore are especially suitable for some constrained environments[14].

2.1 Common Password Generation:

People are notoriously remiss at achieving sufficient entropy to produce satisfactory passwords. Some stage magicians exploit this inability for amusement, in a minor way, by divining supposed random choices (of numbers, say) made by audience members. Thus, in one analysis of over 3 million eight-character passwords, the letter "e" was used over 1.5 million times, while the letter "f" was only used 250,000 times. A uniform distribution would have had each character being used about 900,000 times. The most common number used is "1", whereas the most common letters are a, e, o, and r [9]. Users rarely make full use of larger characters sets in forming passwords. For example, hacking results obtained from a MySpace Equations phishing scheme in 2006 revealed 34,000 passwords, of which only 8.3% used mixed case, numbers, and symbols [10].Note that the full strength associated with using the entire ASCII character set (numerals, mixed case letters and special characters) is only achieved if each character in the password is chosen randomly from that set. Capitalizing a letter and adding a couple of numbers and a special character to a password will not achieve the same strength. If the numbers and special character are added in predictable ways, say at the beginning and end of the password [13], they could even lower password strength compared to an all letter random password of the same length.

2.2 Common Guidelines to generate a Strong Password [13][01][11] :

Guidelines for choosing good passwords are designed to make passwords less easily discovered by intelligent guessing, common guidelines include:

A minimum password length of 12 to 14 characters if permitted.

- ❖ Generating passwords randomly where feasible.
- ❖ Avoiding passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), or biographical information (e.g., ID numbers, ancestors' names or dates).
- ❖ Including numbers, and symbols in passwords if allowed by the system.
- ❖ If the system recognizes case as significant, using capital and lower-case letters.
- ❖ Avoiding using the same password for multiple sites or purposes.

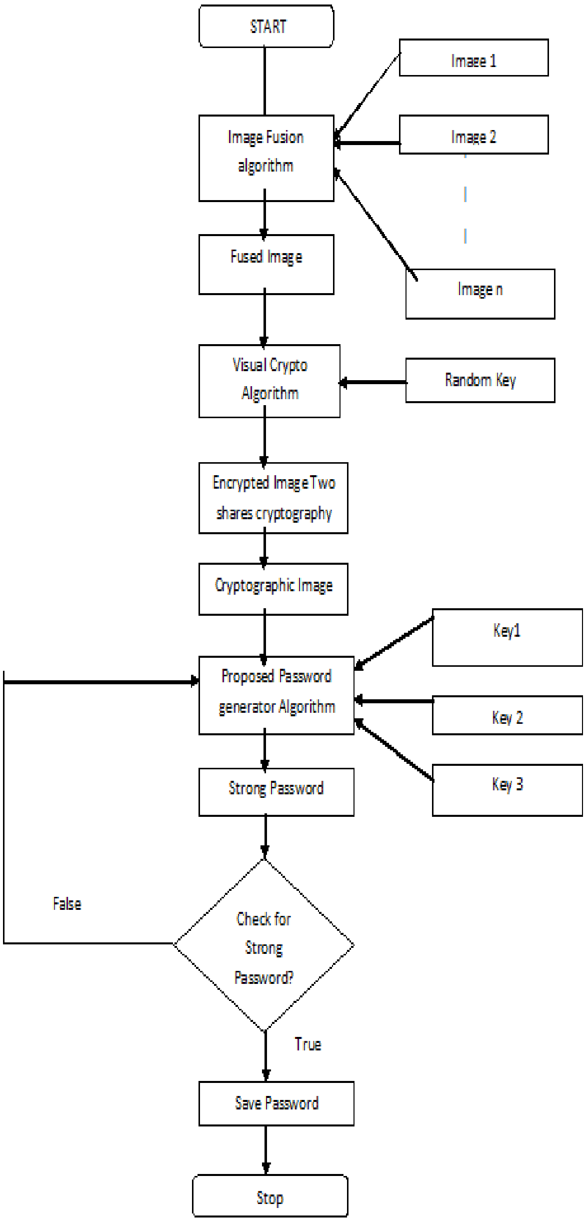
Avoid using something that the public or workmates know you strongly like or dislike. Kept in a safe place, such as a wallet or safe, not attached to a monitor or in an unlocked desk drawer. The possible character set for a password can be constrained by different web sites or by the range of keyboards on which the password must be entered [09].

Existing password-based authentication schemes can be categorized into two types - one uses weak password and the other uses strong-password [1]. The weak password authentication scheme is based on public-key cryptographic techniques and has the advantage that the remote system does not need to keep a verifier table to verify the validity of the user login. Though, weak-password is easy to memorize; however, weak-password authentication schemes lead heavy computational load to the whole application system because of using public-key cryptographic techniques. In contrast, the computational load of most strong-password authentication schemes is lighter because of using only simple operations, e.g., one-way hash function and exclusive-OR operation [2]. The strong-password authentication schemes have another advantage over weak password authentication schemes that their implementations are easier and with less cost. However, a strong-password is difficult to memorize.

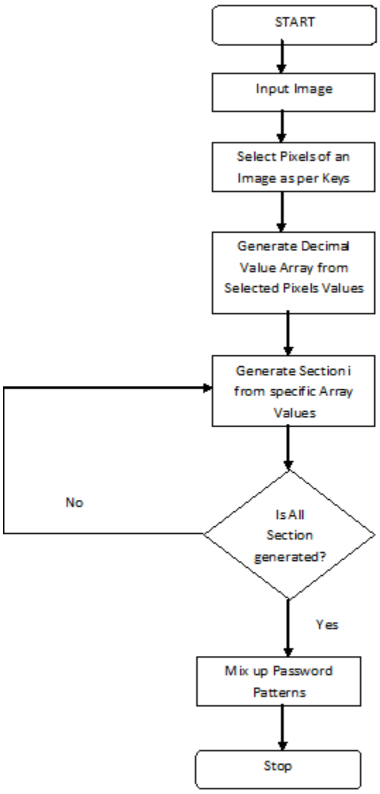
III. Proposed Work Methodology (System Block Diagram)

3.1 Proposed methodology:

3. Proposed Work (Methodology): System Block Diagram



3.1 Proposed Password generator Algorithm


START
Input Image
Select Pixels of an Image as per Keys
Generate Decimal Value Array from Selected Pixels Values
Generate Section i from specific Array Values
No
Is All Section generated?
Yes
Mix up Password Patterns
Stop

3.2 Proposed Strong Password generator system:

3.2 Proposed Strong Password generator system:

To achieve the proposed system, Select input Images (from the array of images) which may be of any type like RGB, Gray and Binary etc. We perform Image fusion algorithm that combines all the selected images into a single Image. Significance of image fusion algorithm is only to avoid the dependency of generated password on a single image. Image fusion modifies input image pixels & at the end result, we find two or more images are mixed up.

Once the images are fused, we will apply two shares Visual Cryptography Algorithm, which encrypt the image & convert it into unreadable format. The Cryptographic image is unreadable in format that’s why an intruder will find difficulty in reading Plain image for password decryption. Cryptographic image contain a decimal pixel value either 0 or 255.

Crypto image is a input to our Proposed Password Generator Algorithm we choose the pixels from Crypto image based on the Key values, we suggest the multiple key selection to create more patterns of selection. Finally we assemble all these selected pixels into a single dimensional array which we will divide into 04 sections that is Numbers, Characters, Special Symbols, & Special Character. Strong password definition says that, “ Password should contain Digits, Characters, Special Symbols, & Special Characters and it should not be breakable by any of the intelligent Intruder easily, in proposed work; we will try to Mix up all the generated sections with permutations so that every time & in every round an Unique Password will be generated. Once the password is generated we pass this password from strong password definition filter if it passes through that than we will use it for the Authentications else we forward it to proposed password generator algorithm again (until it qualifies for the definition of a strong password).

IV. CONCLUSION

Current research work is dedicated to Generate Strong password, using Image Fusion & Two-Share Cryptography. The strength of proposed system lies in a sufficiently large collection of images to avoid short repeating cycles. Compared to other methods reviewed, our system may require human-interaction and careful selection of images. Cryptography also performs significant role to encrypt the resultant fused image, which finally resembles into the password string. This password string will further checked against the definition of strong password & than finally delivered to the deserving authority.

Besides this system, current work can be extended for the proper delivery of the password string to the deserving recipients of it. This task can be accomplished using one of Key Distribution Mechanisms.

REFERENCES

[1] Masayuki Fukumitsu et.al, “A proposal of an associating Image based password Method & a development of password creating support system”, 24th IEEE International Conference on Advanced Information Networking and Applications, 20-23April2010, ISSN 1550-455X.

[2] Burnett, Mark (2006). Kleiman, Dave. ed. Perfect Passwords. Rockland, Massachusetts: Syngress Publishing. p. 181. ISBN 1-59749-041-5.

[3] William e Burr et. al, NIST Special Publication 800-63, version 1.0.2, online available on
URL: http://en.wikipedia.org/wiki/Password_strength.

[4] Burnett, Mark (2006). Kleiman, Dave, ed. Perfect Passwords. Rockland, Massachusetts: Syngress Publishing. p.p 181. ISBN 1-59749-041-5.

[5] Bruce Schneier (December 14, 2006). "MySpace Passwords aren't so Dumb",Wired Magazine, Retrieved April 11, 2008.

[6]Cipresso P, Gaggioli A, Serino S, Cipresso S, Riva G: How to Create Memorizable and Strong Passwords. J Med Internet Res 2012;14(1):e10; http://www.jmir.org/2012/1/e10/

[7]Brumen B, Heričko M, Rozman I, Hölbl M: Security Analysis and Improvements to the PsychoPass Method. J Med Internet Res 2013; 15(8):e161. http://www.jmir.org/2013/8/e161/

[8] Microsoft Corporation, Strong passwords: How to create and use them, online available on http://www.microsoft.com/security/online-privacy/passwords-create.aspx.

[9] Bruce Schneier,
https://www.schneier.com/blog/archives/2007/01/choosing_secure.html

[10] Google Inc. https://accounts.google.com/PasswordHelp

[11] Bidwell, Teri re (2002). Syngress Publishing. ISBN 1-931836-51-5

[12]BruceSchneier,
https://www.schneier.com/blog/archives/2005/06/write_down_your.html

[13] http://thehackernews.com/2011/09/comodohacker-responsible-for-diginotar.html

[14] Jiang Huiping , “Strong password authentication protocols” Distance Learning and Education (ICDLE), 2010 4th International Conference, San Juan, PR, E-ISBN: 978-1-4244-8752-3, PP 50 - 52