Implicit Authentication Approach by Generating Strong Password through Visual Key Cryptography

Dr. Ajay B. Gadicha[1], Dr. Vijay B. Gadicha [2]

[1]Assiatnt Professor, Department of Computer Science & Engg., P.R.Pote C.O.E. & M., Amravati ajjugadicha@gmail.com

[2] Associate Professor, Department of Computer Science & Engg., G.H.Raisoni Academy of Engg. & Tech, Nagpur vijay.gadicha@raisoni.net

Abstract: In this era of digitization where literally everything is available at the tip of the finger. Huge amount of data used to flow day in day out, where users used to work with various applications like internet websites, cloud applications, various data servers, web servers, etc. This paper provide idea about access control or authentication used to be acting as first line of defense for preserving data secrecy and its integrity, so far it is learned that the usual login password based methods are easy to implement and to use as well but it is also observed that they are more subjected to be get attacked therefore to preserve authentication on the basis of simple alphanumeric passwords is a challenging task now a days. Hence new methods which bring more strength for authentication and access control are so very expected and desirable.

Keywords: *Strong password, Image pool, access control, authentication, Image Fusion, Visual Key Cryptography*

1. Introduction

Before visiting various innovative schemes of generating strong password, let's observe the crucial parameters which will determine and demonstrate the effectiveness of a password. There are various factors available which determines the strength of password. The first one is how long the password is in length? If it is too short then it may be easily guessed. Second parameter is doing the password generated in a sequence or they are created randomly. if the password generation is in sequence then once the attacker gets acquainted with the pattern of password generation then it becomes extremely simple for him to crack the password and if it is randomly generated then user must remember it and recollect it as an when required.

The third factor may be considered as how passwords are stored and used. Let us consider that a strong set of passwords are generated but if those are not stored at proper place with certain degree of security then all those passwords may be hacked or leaked, which will cause threat to information security. sometimes the utilization of the password is also becoming case of worry, because if the passwords is too strong that means it may have big length and combination of various alphanumeric characters then it becomes difficult for users to recall and recollect it for using in some application. Therefore, all the above parameters must be kept in mind while designing strong password. Work has to be done by considering above parameters so that we will present a strong password generation model which will provide enough strength and must be recollect and recall wherever and whenever required. This requires a comprehensive study of various security issues which are related to access control and authentication. While creating passwords usually users used to make various mistakes which will ultimately resemble in generation of weak password.

DOI: 10.5281/zenodo.3686195

Some of the example of such passwords which are treated as weak in strength are may be formed due to following reasons.

1. Users may use their name or surname as a password
2. They used their location or address as their password
3. Sometimes they used name of family member or friend or relative as their password string.
4. Sometimes user chooses vary common names which are used in day to day life to suit them as their password.
5. Various times it is observed that user use to put their password as their mobile number, roll number or some registration number which is easily available with everyone.
6. It is also observed that various times user use to put the name of god or some famous personality may be their idle person as their password.

All the above attributes which are enlisted will bring the chances of password hacking for any arbitrary user therefore while choosing a password for any specific application a user must take care that he/she must not select password which contain above attributes. Some of the desirable attributes which are expected to create a strong password string are given below: -
1. The size of the password string should be minimum eight to fifteen characters.
2. It must have involvement of uppercase letters like A, B, …, Z
3. It should contain lower case letters a, b……z.
4. It should have numbers in it like 0, 1, 2…….9.
5. It must have some of the special symbols like @, $, #, *, /, ^, %, <, >,, + , - , { , } , [,].
Hence if the user follows the above-mentioned attributes to generate the strong password then it is obvious that the resultant password will be strong and it can't be easily guessed by attacker, by using various attacking tools or some automated procedures in stipulated time duration. But to have various strong passwords for various user application which user use to have in daily life is really a challenging task therefore a process has to be identified which will provide sufficiently strong password to all the users to satisfy their requirements.

1.1 Need of Image Based Password: -

Currently, as information systems are more open to the Internet, the importance of security for networks is tremendously increased. Usable security has unique usability challenges because the need for security often means that standard human-computer interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. So, researchers of modern days have been found alternative technique to secure our confidential data from attacks. It is now beyond any doubt that user authentication is the most critical element in the field of Information Security. The simplest & easiest method used is textual (alphanumeric) passwords for securing the confidential data. These types of passwords are strings of letters and digits, but there are several deficiencies in these textual passwords. In this technique passwords used are short and simple which are easy to remember, So textual passwords can be personal names of family members, dictionary words, birth - date, pet name, phone number etc. and vulnerable to various attacks like dictionary attack, easy to guess, key - loggers, shoulder surfing, social engineering, spyware attack, hidden camera etc. Also, now users require the passwords for personal computers, social networking, emails and many more applications, and for all these systems to remember easily the users can use the same password which reduces security. So, in this way if textual passwords are kept difficult then they are difficult to remember and if kept easy then they are easy to guess.

DOI: 10.5281/zenodo.3686195

Text Based Password Authentication (TBPA) has shown some difficulties that users have tended to write passwords down manually or save them on hard disc. Graphical User Authentication (GUA) has two symbiotic pillars as its foundation: USABILITY & SECURITY. The macro-concept of GUA is based on the human psychological factor that is images are more readily committed to memory than would TBPA‟s.
Therefore in the proposed work, a sufficiently large pool of images is taken into the consideration to generate the password string. Here from this pool of images arbitrarily any random number of images may be selected which will reduce the dependency of creating a password on single image or repetitive pattern/sequence of images. These arbitrarily selected images will be given as an input to an image fusion algorithm which will fuse these images and results in a fused image. Later this fused image will be encrypted by using Multi-share Visual cryptography mechanism to produce an encrypted image. Further this encrypted image will be mixed with an audio file (.wav) format to finally produce the resultant cryptic image from this resultant image multiple shares can be obtained. Out of these multiple shares one of the shares will be chosen at random for generating the strong password from its Corresponding pixel values.

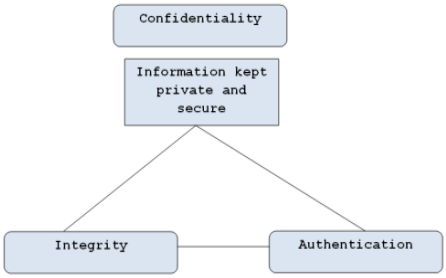

Fig 1: Parameters of Information Security

1.2 *Visual Key Cryptography:*

Visual cryptography may be performed on this fused image (say C) to convert it into its cryptic image so that the internal information (like pixel values) of that image will no longer accessible to any programmer or intruder.

1.3 *Overview of Strong Password Generation Using Images: -*

From the above discussion it was observed that image based password happens to be more suitable and secure in compared to usual text based password but simply keeping an image as password or some information regarding that image like some name or some attribute of an image placing as password will enhance the dependency of the password over a single image which is completely undesirable.
Therefore, in the proposed work, a sufficiently large pool of images is taken into the consideration to generate the password string. Here from this pool of images arbitrarily any random number of images are selected which will reduce the dependency of creating a password on single image or repetitive pattern/sequence of images. These arbitrarily selected images will be given as an input to an image fusion algorithm which will fuse these images and results in a fused image.
Later this fused image will be encrypted by using Multi-share Visual cryptography mechanism to produce an encrypted image. Further this encrypted image will be mixed with an audio file (.wav) format to finally produce the resultant cryptic image; now from this resultant cryptic image's multiple shares can be obtained. Out of these multiple shares one of the shares will be chosen at random for generating the strong password from its corresponding pixel values.

DOI: 10.5281/zenodo.3686195

The rest of this paper is represented as follows; Section 2 represents related work, Section 3 introduces techniques used in our research, Section 4 represents proposed technique used for generating strong password, and Section 5 represents experimental results and Discussion.

2. RELATED WORK

This chapter brings the brief literature survey related to the proposed work. It initially provides fundaments of information security and also narrates its importance to the present communicating scenario. Then this gives the basic information about the Authentication and Access control, various methods have been discussed here for establishing the authentication between the two communicating parties.

[Zhenfeng Shao and Jiajun Cai, 2018] Remote sensing images with varying spatial and spectral resolution, such as panchromatic (PAN) images and multispectral (MS) images, can be obtained by many earth-observing satellites. Normally, PAN images possess high spatial resolution but low spectral resolution, while MS images have high spectral resolution with low spatial resolution.

[Sadiq Almuairfi et al., 2011] proposed idea about implicit password authentication system is used for protecting confidentiality and integrity of the data. Here graphic based password is generated. In this scheme during registration server will request the user for generating a piece of information which is used for the password.

[Hung-Min Sun et al., 2012] proposed that the most popular technique used by the user is text-based password which provides the more convenience and simplicity. Most of the time users use the same password on different websites for different accounts. Due to which it can be easily crack by hacker. Again, domino effect is caused due to consistently reusing the password. So, to protect different types of attacks used by the hacker for stealing password new technique is introduced as oPass authentication protocol which is going to resist any stolen attacks and reusability passwords attacks.

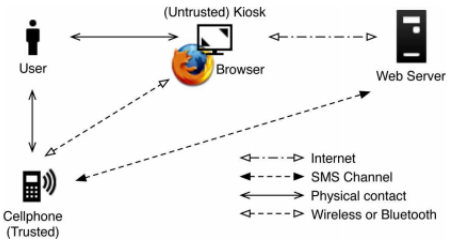

Fig 2: Working of oPass

[Fourozan, 2010] Basically, Cryptography is a technique in which known plain text can be converted into some Cipher text by using encryption algorithm and appropriate key value. These cipher texts are formed to ensure the secrecy and confidentiality of the information. Because the cipher text generated after the implementation of cryptography is not easily understandable, actually it's a meaningless text which is encrypted by using some algorithm.

[Bin Yu et al., 2007] When there is a need to share more than one secretes image then original visual cryptography scheme (VCS) fails, because at a time only single image can be shared by the original VCS. So, whenever there is need to share more secrete images for that there is a need to preserve a number of shares which increase our burden. A multi-secrete sharing threshold visual cryptography scheme is proposed which is based on (k, n)-VCS and that participant preserves a share to share more than one secretes image and also expands the scope of application.

[Xiaotian Wu and Wei Sun, 2013] There is one method which used to implement visual key cryptography without doing any pixel expansion that is the Random grid (RG) method. In Random grid based visual cryptography due to the average light transmission of share is fixed at (1/2) because of which

DOI: 10.5281/zenodo.3686195

the lower visual quality of reconstructed secret image is reveal. In this proposed work, the concept of generalized Random grid was introduced, in which the light transmission of shares becomes adjustable, and also for implementation of different VC schemes generalized RG methods were adopted.

[Yanyan Han et al., 2014] A new digital watermarking algorithm of color image has proposed here. After processing a watermark, based on visual cryptography two shares are generated. One of them is protected by the copyright and another one is embedded into a color image. The proposed scheme is easily implacable and highly feasible. The robustness and the embedding capacity of watermark can be improved effectively using this mechanism.

dataset given as input to the network and 30% of the dataset is given as unseen to the network. The implemented network gives the error rate at 0.0773 of MSE and the accuracy as 90 % [10].

3. TECHNIQUES USED

3.1 Implementation of Proposed Methods:

A) *Multi-Image fusion*:

Image fusion is the process in which two or more images will be combined together to form a fused image. While performing the fusion of the images it must be taken care that both the images which are going to be fused must are of same size. If images do not belong to same size then the influence of smaller image remains less in the resultant fused

image therefore to maintain the equal influence of all the images which are participating in fusion process must be taken of same size.

When one image will be joining with another image then its pixel values will be combined with each other. The fusion of the two images will take place pixel by pixel merging from two images. To initiate the process of image fusion it is needful that at a time only two images can be fused. if there are more than two images to fuse then initially two images will be fused afterwards the resultant fused image will be further fuse with the next image and so on. The below diagram broadly provides the way of fusing the images when there are multiple images are available to fused.

B) Pixel-wise Image fusion Process:

It is clearly known that a pixel is a smallest unit available in an image. If the image is of RGB model (for example) then the corresponding pixels of the image carries Red Green and Blue values in it. Each pixel carries a value of 24 bits, where 8 bits are dedicated to red color next 8 bits are to green color and last 8 bits are to blue color respectively.

Fig 3: Representation of single pixel of RGB image.

Image Fusion Algorithm:

1. Start
2. Input Image1 I1 and Image2 I2
3. If Size(I1) != size(I2)
   goto step 6
4 for i= Height(I1)
   for j=Width(I1)
   p = I1(i, j) & q = I2(i, j)
   Extract R, G, B from p and q;

FR = RpMSB || RqMSB

DOI: 10.5281/zenodo.3686195

FG = GpMSB || GqMSB
FB = BpMSB || BqMSB
end
end
5. Save Fused Image IF.
6. Stop.

3.2 Visual Key Cryptography:

the fusion of various images has been performed by combining their content part so that the influence of all the images will remain in the fused image. Now here once all the images are fused then visual key cryptography (VKC) will be performed on the obtained fused image. Consider the fused image available in RGB format, as this image contains pixel values for red color, green color and blue color having values from 0-255. Now let us first extract Red, Green, and Blue contains of image separately which will be done by extracting only one color active out of three colors. So here three shares will be obtained where first share contains only red color, next contains only green color and final shares contains only blue color.

VC Algorithm

1. Start
2. Input Fused Image F.
3. Create Three Blank Shares R1, G1, B1 with (Width(F), Height(F))
4. For i=0 to Width(F)
For j=0 to Height (F)
Read Pixel at P (i,j)
Extract R G B from P (i,j)
Set
R1 (i, j) = (R, 0, 0)
G1 (i, j) = (0, G, 0)
B1 (i, j) = (0, 0, B)
End
End
5. Save R1, G1, B1 Shares
6. Stop.

In above algorithm initially consider the fused image; from this fused image 03 shares are going to be derived. For that first of all create 03 blank shares as R1, G1, and B1 with same width & height of fused image. Now read each pixel value p (i,j), as these values corresponds to Red, Green & Blue values.

D) Mixing of audio samples in cryptic image (.wav format):

From above module of VKC the cryptic image was obtained. This image possesses maximum Mean Square Error (Value) to that of initial fused image. The cryptic image must remain very deceptive for any intruder or hacker who wants to hack or crack the system; therefore, in this obtained cryptic image an audio wave file is to be mixed to enhance the complexity for the intruder to crack the password generation. To do that, let's consider an audio wave file which is available in various audio samples.

DOI: 10.5281/zenodo.3686195

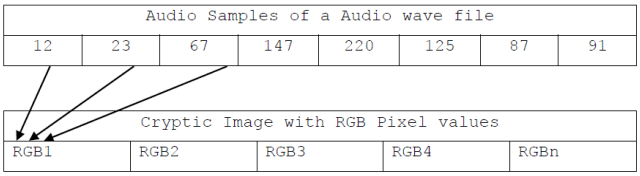

Fig 4: Mixing of Audio Sample

As per the above given figure, the first 03 samples of audio wave file that is 12, 23 & 67 are replaced with first pixel's Red, Green and Blue values respectively. This replacement will carry on until the resultant file containing cryptic image & audio sample will be obtained. While replacing the audio wave sample values with the pixel values of Red, Green & Blue it is to be seen that, if the pixel value of Red or Green or Blue is 255 or zero, than these pixel values must not be replaced by audio samples, rather these value are converted in the range as not equal to zero or not equal to 255

3.3 Image classification upon its pixel values:

The resultant file is obtained which influence of cryptic image has formed after performing visual key cryptography on fused image and an audio wave sample file. Now this resultant cryptic file appears again as an image which contains various pixel values in two-dimensional array format. As each pixel contains it's red, green, and blue components in it, therefore upon the decimal value of the red, green and blue component they will be distributed to various classes of ASCII characters. The total range of ASCII characters which is used here is from decimal 32 to decimal 127. In this range only all the red, green, and blue color component values are assigned to various classes ASCII Characters

Image classification Algorithm
1. Start
2. Input Resultant Cryptic Image file Ci
3. For i=0 to Width (Ci)
For j=0 to Height (Ci)
Read Pixel P (i, j)
Extract Component Crgb from P(i, j)
If (Crgb >=n1 && Crgb <=n2)
Add Crgb to Class A
End
If (Crgb >=n3 && Crgb <=n4)
Add Crgb to Class B
End
If (Crgb >=n5 && Crgb <=n6)
Add Crgb to Class C
End

If (Crgb >=n7 && Crgb <=n8)
Add Crgb to Class D
End
If (Crgb >=n9 && Crgb <=n10)
Add Crgb to Class E
End
If (Crgb >=n11 && Crgb <=n12)
Add Crgb to Class F

DOI: 10.5281/zenodo.3686195

End
If (Crgb >=n13 && Crgb <=n14)
Add Crgb to Class G
End
End
End
4. Save Class A, B, C, D, E, F, G
5. Stop

F) Strong Password Generation:

To generate strong password, let's first reanalyze the definition of strong password. A strong password must be of suitable length minimum (06 to 08) characters. These characters contain capital letters, small letters, operators, special symbol and special characters in it. So, to generate such a kind of password string, let us consider the 07 classes of ASCII characters as per the ASCII chart, all these 07 classes contain the occurrences of capital letters, small letters, special symbol and special characters. Hence the password string formed from them will be indeed going to be strong password string.

Now to generate the strong password string let us consider the following figure which demonstrates the working methodology for generating the strong password. In this various classes of ASCII characters are formed according to their ASCII values and all these classes will correspond to form the strong password string.

Strong Password Algorithm:

1. Start
2. Read Classes A,B,C,D,E,F,G
3. Set index i=0, Password=" ";
4. Input Password Length (PL)
5. For i=0 to PL
Read Ch=A(i)
Password = Password + Ch;
i++;
Go to step 6
Ch=B(i)
Password = Password + Ch;
i++;
Go to step 6
Ch=C(i)
Password = Password + Ch;
i++;
Go to step 6
Ch=D(i)
Password = Password + Ch;
i++;
Go to step 6
Ch=E(i)
Password = Password + Ch;
i++;
Go to step 6
Ch=F(i)
Password = Password + Ch;

DOI: 10.5281/zenodo.3686195

i++;
Go to step 6
Ch=G(i)
Password = Password + Ch;
i++;
Go to step 6
6. If(Length(Password)>=PL)
Go to step 7
Else
Return;
End
7. Save Password
8. Stop

4. PRPOSED TECHNIQUE

To achieve the proposed research work, select input Images (from the array of images) which may be of any type like RGB, Gray and Binary etc. Then to all these selected images, Image fusion algorithm is performed that combine 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 & ultimately a fused image is obtained which is combination of multiple images. This fused image has the influence of all images in it.

Once the images are fused, Visual Cryptography Algorithm is applied on it, which encrypts the image & converts 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 contains a decimal pixel value either 0 or 255.

Now this cryptic image is given as an input to audio mixing process where a .wav audio sample file will be mixed with the cryptic image. Finally, the resultant file will be obtained, this resultant cryptic image file act as an input to proposed Password Generator Algorithm. Here chosen pixels values from resultant cryptic image file are collected based on the classification of image pixel values. Finally, all these selected pixels values are assembled into a single dimensional array which we will divide into various sections that is Numbers, Characters, Special Symbols, operators & 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, an attempt is made to Mix up all the generated sections with permutations so that every time & in every round a Unique Password will be generated. Finally, once the password is generated than this password will be checked against strong password definition, if it passes through that than this will be used for the user Authentications.

The proposed password generation mechanism is free from the patterns of alphanumeric letters or symbols also it is not relying heavily on any single image or set of images. As every time when user want to generate a password string, he/she can choose any numbers of arbitrary images and for every iteration new set of images can be chosen as an input to password generation process. Here in the proposed method the privilege is given to the user to select the numbers of passwords he/she wants to generate by following the mentioned sequence of various algorithms.

It is very difficult for an intruder to crack the password string generated by this unique process, because the hacker must know the set of images used in the process as well as their sequence while they are fused with each other. Also, there is involvement of various key values at some important algorithms without which a hacker can't reconstruct the password string. Additional to that an audio (.wav) file is also mixed with the cryptic image which will make it more difficult for any intruder or hacker to predict the

DOI: 10.5281/zenodo.3686195

inputs used for the password generation process. Figure given ahead explains the flow of the complete process.

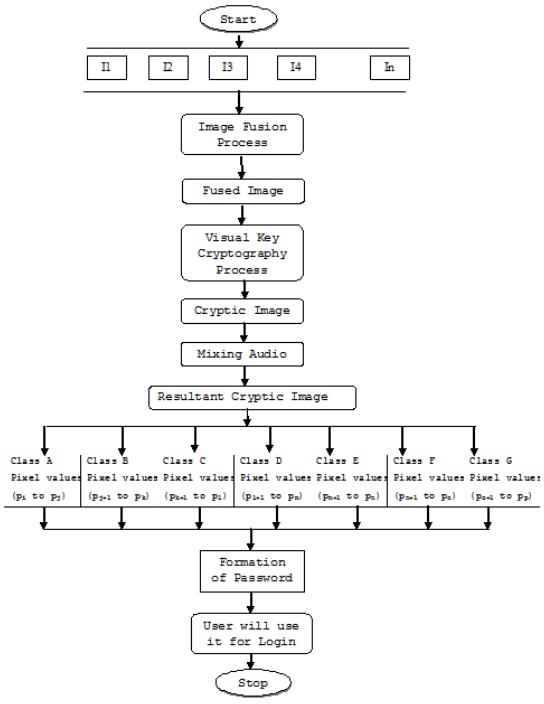

Fig 5: Proposed Working

In above given figure 2, it is clearly observed that the proposed method is free from the dependency on any single image as any number of arbitrary images can be selected for fusion from a given pool of images. Then all those images will be fused by using the content part of the images. On this fused image visual key cryptography is performed to obtain a cryptic image later in this cryptic image an audio wave file is merged to make it more deceptive for the intruder or hacker. Finally, this resultant file will be classified according to its pixel values and from this classification the password string is generated. Further this generated password will be checked for its strength if this turns out to be strong password then will be provided to user for login purposes which will ultimately help to preserve user authentication/access control.

V. RESULT AND DISCUSSION:

Fundamentally the result analysis is accomplished on some of the crucial quantitative parameters associated to image fusion, visual key cryptography and determination of password strength. Finally, chapter ends with the detailed comparative analysis performed between the existing systems & the proposed work

1. Analysis on quantitative parameters for image fusion process:

DOI: 10.5281/zenodo.3686195

Sr. No.	Name of Input Image	Entropy	Mean	Standard Deviation	Height & Width
1	CARS_28.JPG	6.681	54.17	62.29	400*2160
2	CARS_72.JPG	6.542	83.17	53.80	600*2400
3	CARS_35.JPG	7.52	79.16	71.60	480*1920
4	CARS_50.JPG	7.02	61.26	68.71	500*2400
5	CAR2.JPG	4.53	184.73	90.36	480*1920
6	CARS_31.JPG	7.36	131.27	72.80	469*1911
7	TTROADSTERS.JPG	7.65	96.33	63.30	250*1320
8	CARS_45.JPG	7.44	114.31	46.23	492*2214
9	CARS_40.JPG	7.79	119.82	82.46	480*1920

Table1: Parameter-wise Result Orientation

Password Key	Length	Special Symbols	Digit	Operator	Upper Case	Lower Case	Other	Iteration	Generation Time (ms)
"3?G'd|,3@	10	3	2	2	1	1	1	1	46.8001
#4@Hae}-A4	10	2	2	1	2	2	1	2	0
$5AIbf~5.B	10	2	2	0	3	2	1	3	0
%6BJcgl6C/	10	2	2	0	3	2	1	4	0
&7CKdh-D70	10	1	3	0	3	2	1	5	0
"3?G`d|@,3	10	3	2	2	1	1	1	6	0
#4@Hae-}4A	10	2	2	1	2	2	1	7	0
$5AIbf.~B5	10	2	2	0	3	2	1	8	0

Table2: Contents of Strong Password String

Above data table provides the details of all the 10 images which are used for image fusion. The quantitative parameters used are Image Entropy, Mean of an Image, Standard deviation, and height & width of an image. Where entropy quantities provide the details of data contain by the image, mean gives the mean value of image pixels (which is going to be between 0 to 255), standard deviation provides the difference between the pixel values and height & weight provides the actual size of an image. Further all these image properties are analyzed in details

5. Conclusion

Current research work is dedicated to Generate Strong password, using Image Fusion & visual Cryptography. The strength of proposed system lies in a sufficiently large collection of images to avoid short repeating cycles. Compared to other methods reviewed, proposed 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 strong password string. These passwords will provide strength to the information security mechanism specially related to authentication & access control.

References

[1] Zhenfeng Shao, Jiajun Cai, "Remote Sensing Image Fusion With Deep Convolutional Neural Network", IEEE Transactions on Applied Earth Observations And Remote Sensing, DOI 10.1109,ISSN: 1939-1404, 2018.

[2] Sadiq Almuairfi, Parakash Veeraraghavan and Naveen Chilamkurti, "IPAS: Implicit Password Authentication System", IEEE International Conference on Advanced Information Networking and Applications, 2011.

[3] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", vol 7, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, April 2012.

[4] Forouzan and Mukhopadhyay "Cryptography & Network Security", McGraw Hill India Press, 2010, pp 381-383.

DOI: 10.5281/zenodo.3686195

[5] Bin Yu, Xiaohui Xu, Liguo Fang "Multi-secret Sharing Threshold Visual Cryptography Scheme", IEEE International Conference on Computational Intelligence and Security Workshops, 2007.

[6] Xiaotian Wu and Wei Sun, "Generalized Random Grid and Its Applications in Visual Cryptography", IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 9, SEPTEMBER 2013.

[7] Yanyan Han, Wencai He, Shuai Ji, Qing Luo, "A Digital Watermarking Algorithm of Color Image based on Visual Cryptography and Discrete Cosine Transform", International Conference on P2P, Parallel, Grid, Cloud and InternetComputing2014.

[8] Ajay B. Gadicha ,M.V. Sarode "A Review on Video Security Using Visual Cryptosystem" Journal Procedia Computer Science ,Volume 78 Issue C, March 2016 Pages 729-733..

[09] Mr. Ajay B Gadicha, Dr. M.V.Sarode, Dr. V.M.Thakare, "Design Prognostic Framework for Scene Classification in VideoProcessing" International Conference on Physics and Photonics Processes in Nano SciencesJournal of Physics: Conference Series1362 (2019).

[10] Ajay B Gadicha ; M.V. Sarode ; V.M. Thakare, "Aggregating and Searching frame in Video Using Semantic Analysis" 2018 International Conference on Advanced Computation and Telecommunication (ICACAT) 28-29 Dec. 2018.

[11] Dougal Maclaurin.Modeling, Inference and Optimization with Composable DifferentiableProcedures. PhD thesis, Harvard University, April 2016.

[12] Ajay B Gadicha, M V Sarode and V M Thakare, "Mechanism of Recognizing Key Frames and Scene in Video Using SFT and Classifier Algorithm" Series: Volume 8 Issue 2"Guru Nanak Publications ISSN: 2249-9946.

[13] Ajay B. Gadicha ; M.V. Sarode ; V.M. Thakare," Empirical Approach Towards Video Analysis Using Shot Frontier Detection and Key-Frame Mining" IEEE 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS).

[14] Vijay B Gadicha ; A. S. Alvi, "Extensive Approach for Strong Password Generation Using Content-Color Mechanism" 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA).

[15] Vijay B. Gadicha , A. S. Alvi "A Novel Approach towards Authentication by Generating Strong Passwords" Proceeding ICTCS '16 Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies Article No. 69 Udaipur, India — March 04 - 05, 2016.

DOI: 10.5281/zenodo.3686195