ISSN 2395-1621

Image based authentication one time Password

[#1]Puja Bharti, [#2]Apeksha Hipparkar,[#3]Nisha Patil, [#4]Namrata Kadam,[#5]S.P.Patil

[1]puja24.bharti@gmail.com
[2]apekshahipparkar11@gmail.com
[3]nishasbliss@gmail.com
[4]namratak64@gmail.com
[5]shivprasad.patil@sinhgad.edu

[#1234]Department of Information Technology,NBN Sinhgad School Of Engineering,Pune,India-411041
[5]Professor,Department of Information Technology,NBN Sinhgad School Of Engineering, Pune,India 411041

ABSTRACT

In this paper, a novel image watermarking algorithm based on visual cryptography (VC) is presented. Keyboard tracing and screen capturing is a serious security threat to Internet users and is a fraud in which the perpetrator trace the keyboard to hack in order to gather personal and financial information of the receiver. It is important to prevent such attacks. One of the ways to prevent the password theft is to avoid using text passwords and to authenticate a user with image password. Image based authentication one time password is one of the important way to provide more security to the system. Here, we are using image as a password and applying visual cryptography and watermarking on it to make it more secure as well as one time password is also generated to make it more secure. Using the immediate messaging service available using internet, user will obtain the One Time Password (OTP) after image validation. This project integrates Image based authentication and one time password to get high level of security in authenticating the users over the internet.

ARTICLE INFO

Article History

Received :3rd March 2016

Received in revised form :

4th March 2016

Accepted : 6th March 2016 ,

Published online :

9th March 2016

***Keywords*—** Image watermarking, visual cryptography, One Time Password, Security.

I.INTRODUCTION

Nowadays, with the development of internet network and digital technology around the world, the availability and usage of digital information has increased quickly. People can process, exchange and store digital contents more simply than ever. However, against this advantage, a new set of problems concerning security such as unrestricted duplication, manipulating and distributing of multimedia have arisen. Therefore, ownership protection and content verification have become a significant issue. Among the existing techniques to solve these problems, watermarking is considered as a strong technique [1].

In this internet era security require more attention so, there are several techniques used for security. For security purposes text data converted into image. So, there must be more concerned about security of images [2]. Digital watermarking is a process of embedding digital information called watermark into the digital multimedia data. Watermarking technique is used for several purposes including content authentication, owner identification, data integrity and copy control.

This technology is an emerging field in computer science, cryptography, signal processing and communication. Digital water-marking is intended by its developers as the solution to the need to provide the value added protection on top of data encryption and scrambling for content protection. In general a digital watermark is a procedure which allows an individual to add hidden copyright information or other verification message to digital media. The watermark may be a logo, label or a random sequence. A typical good watermarking scheme should aim while keeping the

embedded watermark very robust under malicious attack in real and spectral domain.

Image Based Authentication:

Image Based Authentication is used for applying One Time Password (OTP) to provide more security of user's personal account with the username and password providing a suitable image for authentication. Image authentication is using the database in a pixel format and application process will be written in Java.

We are using the concept of visual cryptography and watermarking in Image Based Authentication One Time Password.

Visual Cryptography:

Visual Cryptography is an encryption technique to hide information in images in a way that it can be decrypted by the human if the correct key image is used. Visual cryptography is a cryptographic method which allows visual information (pictures, text, etc.) to be encrypted and decrypted using algorithms.

K-N Sharing:

It is an encryption process which is a form of secret sharing, where a secret image is divided into n parts, giving each participant their own unique part, where some of the part or all of them are needed in order to reconstruct the secret. The source image is divided into n shares using k-n secret sharing algorithm using visual cryptography scheme such that all n number of shares are needed to reconstruct the secret image. In this algorithm we can split the image into two or more parts. This is done for security purpose. For secure authentication we have to combine all the parts. Even if one of the parts is hacked, hacker will not be able to authenticate and this is the beauty of K-N sharing algorithm.

Watermarking:

Digital watermarking is a viable solution to the needs of copyright protection and authentication of multimedia data in a networked environment, as it makes possible to identify the author, owner, distributor or an authorized consumer of a document. digital image watermarking that does not need the original image for watermark detection. Here we are using DCT (Discrete Cosine Transform) algorithm for watermarking of image. Watermarking provides special security as the watermarking image is imposed on secret image.

- Discrete Cosine Transform (DCT) :

Discrete Cosine Transform is related to DFT (Discrete Fourier Transform) in a sense that it transforms the time domain signal into its frequency components. The DCT however only uses the real parts of DFT coefficients. In terms of property, the DCT has a strong energy compaction property and most of the signal information tends to be concentrated in few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate as well as remove insignificant high frequency components in images.

De-watermarking:

It is a decryption process for getting the secret image from the watermarked image. The algorithm that we are using for decryption is IDCT (Inverse Discrete Cosine Transform). This requires the watermarked image to separate the secret image from watermarked image.

K-N Merging:

It is a process that comes under the decryption and is used for merging the different shares of image that has been separated during K-N sharing algorithm. Successful authentication is possible only when n shares are combined using K-N merging algorithm.

II.MATERIALS AND METHOD

- Technologies Used:

During the solution development, following soft-wares were used:

- JDK 1.6 (Java Development Kit)
- Net Beans 8.0.2

The system needs the following specifications:

- Hardware Requirement:
  - System : Compatible desktop
  - Hard Disk : 160GB or more
  - Dual core processor
  - RAM : At least 2 GB RAM
- Software Requirement:
  - Operating System : Windows 7 or higher versions
  - Coding language : Java 7.0
  - Database : MySQL 6.3

Stepwise flow of Methodology:

Step 1**:** Enter the confidential data and image during sign up.

User enters the personal details and also selects one image for future generation password .server firstly divides the image into two shares by using k-n sharing algorithm, after that it combines the shares and apply watermarking i.e. DCT (Discrete Cosine Transform) algorithm on it.

Step 2: Secret sharing technique:

Secret Sharing technique is mostly used in distributing sensitive information among specific people. In this technique an images is divided into two shares.

Step 3: User try to login into his/her account.

User logins into his /her account and requests for generation of the password. Server adds one context layer of date/time on the watermarked image and sends it to the user's registered mail .This process repeats every time user tries to login into his account as it provides more security for the user .

Step 4: Image validation Phase.

During image validation, server extracts the context layer from the watermarked image and validates it. If the validation is done successfully, user gets OTP (One Time Password).

Step 5: Login completion phase.

After proper image validation, user gets OTP (One Time Password) on his registered mobile number. User enters one time password, after its validation user logins successfully to his/her account.

- The interaction as well as the communication of the user with the application can be shown with the help of following diagram :

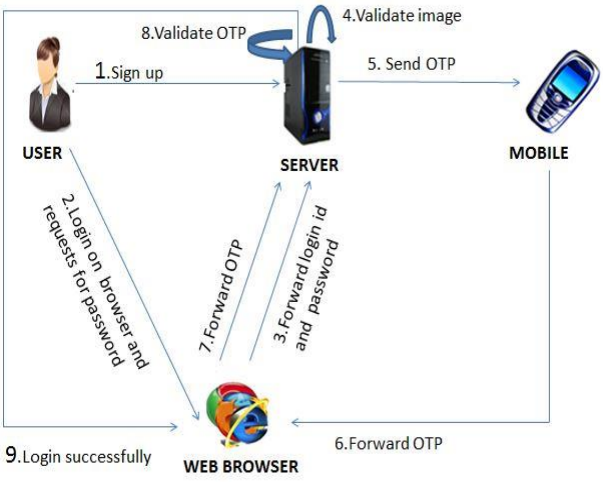

Fig.1: Architecture of IBAOTP (Image Based Authentication One Time Password)

- Mathematical Model :

Set Theory Analysis:

a. Let 'S' be the System
S = {…….}

b. Identify the inputs as C, P and M.
S = {I, P, Y, R, W …}
1. Let I is the set of Images
I = {I1, I2, …. In}
2. Let P is the set of shares stored with server
P= {P1, P2, …. Pn}
3. Let 'Y' is the set of shares stored with user
Y = {Y1, Y2, … , Yn}
4. Let R is the set of secret images
R = {R1, R2, … , Rn}
5. Let 'W' is the set of images generated after Watermarking.
W= {W1, W2, … , Wn}

c. Identify the outputs as O
S = {I, P, Y, R, W …}
1. Let I is the set of Images
I = {I1, I2, …. In}
2. Let P is the set of shares stored with server
P= {P1, P2, …. Pn}
3. Let 'Y' is the set of shares stored with user
Y = {Y1, Y2, … , Yn}
4. Let R is the set of secret images
R = {R1, R2, … , Rn}
5. Let 'W' is the set of images generated after watermarking
W= {W1, W2, … , Wn}

Hence the functionality can be shown as,

- Encryption :
F1: KN sharing
F2: Watermarking

- Decryption
F3: Dewater marking
F4: KN share merging

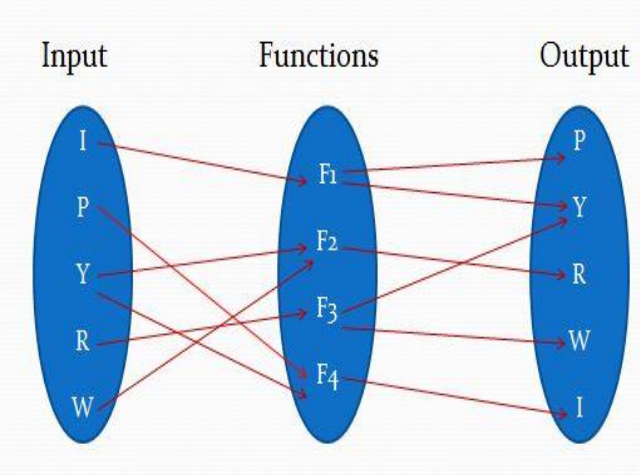

Fig.2: Function Representation in set

III.RESULTS / DISCUSSION

The k-n sharing as well as watermarking algorithm i.e. discrete cosine transform has been applied in the system successfully. One of the experimental results of the k-n sharing is that it makes two shares of images after image insertion process. After that it merges the shares and applies

watermarking on it. During login phase, after image validation, OTP (One Time Password) is generated and verified.

IV.CONCLUSION

In this paper, the system designed is very useful, reliable and user friendly. User can register for the security purpose. As splitting of image password is reducing the hacking due to K-N secret sharing scheme and watermarking DCT and IDCT (Inverse Discrete Cosine Transform) concept is also providing an extra security. After the image validation, OTP (One Time Password) is generated and is successful login occurs due to which our system is getting more layers of security .This project has made us require a professional outlook towards problem statement and solving it to its best and maximum.

REFERENCES

[1] Ali Fatahbeygi, Fardin Akhlaghian ,"A New Robust Semi-blind Image Watermarking Based on Block Classification and Visual Cryptography", 978-1-4799-8445-9/15/$31.00 ©March 2015 IEEE.

[2] Hirdesh Kumar, Awadhesh Srivastava , "A Secret Sharing Scheme for Secure Transmission of color images ", 978-1- 4799- 2900-9/ 14 / $31.00 © 2014 IEEE , pp. 857-860.

[3] Piyush Harsh, Richard Newman, "Usability and Acceptance of UF-IBA and Image Based Authentication System", Proceedings of IEEE ICCST-2007, CISE DEPT, University of Florida, Gainesville FL 32611-6120.

[4] C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithm and application", IEEE Signal Processing Magazine, vol. 18, no. 4, pp. 346,2001.

[5] Bhupendra Ram,"Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 19 ISSN 2278-7763.

[6] Shyong Jian Shyu and Ming Chiang Chen,"Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures" IEEE Transactions on Circuits and Systems for Video Technology, 10.1109/TCSVT.2015.2389372.

[7] Xiaofeng Wang, Kemu Pang, Xiaorui Zhou, Yang Zhou, Lu Li, and Jianru Xue, "A Visual Model-Based Perceptual Image Hash for Content Authentication", IEEE Transactions On Information Forensics And Security, Vol. 10, NO. 7, July 2015.

[8] Arash Habibi Lashkari, Azizah Abdul Manaf, Maslin Masrom, "A Secure Recognition Based Graphical Password by Watermarking", 2011 11th IEEE International Conference on Computer and Information Technology.

[9] Devashish Kumar , Amit Agrawal , Puneet Goyal , "Efficiently Improving the Security of OTP ", 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) .

[10] Hao Luo, Jeng-Shyang Pan, Zhe-Ming Lu, Bin-Yih Liao, "Watermarking-Based Transparency Authentication in Visual Cryptography", 0-7695-2976-3/07,2007 IEEE DOI 10.1109/ISDA.2007.123.

[11] S.Premkumar, A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 978-1-4673-0210-4112/20 12 IEEE.

[12] Mrs.D.Mathivadhani, Dr.C.Meena, "Biometric based authentication using wavelets and visual cryptography", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.

[13] Hae Yong Kim, "A new public-key authentication watermarking for binary document images resistant to parity attacks", 0-7803-9134-9/05/©2005 IEEE.

[14] M.Desiha, Vishnu Kumar Kaliappan, "Enhanced Efficient Halftoning Technique used in Embedded Extended Visual Cryptography Strategy for Effective Processing", 2015 International Conference on Computer Communication and Informatics (ICCCI -2015).

[15] Jinwei Wang, Shiguo Lian, Zhongxuan Liu, Zhen Ren, Yuewei Dai, Haila Wang, "Image Watermarking Scheme Based on 3-D DCT", 0-7803-9514-X/06/©2006 IEEE .