Image with Data Authentication & Compression using Visual Encryption & Huffman Coding

Waseem Ahmad
Gautam Buddha University Greater, Noida, India

Abstract— Due to emerging growth of internet day to day authentication is most important concern today because each and every person are using internet. So authentication is needed today. In security frameworks, data covering up is an expansive teach that incorporates an exhaustive scope of a several research areas. In authentication system we use visual encryption and Huffman coding that contain two scheme firstly data with image split with two share, share1 and share2. First share is store in server database and second share is store in warehouse where authentication is uses. During authentication phase image along with data will display when two share are available at same time. Image can be the fundamental goal of the picture compression is to demonstrate a picture in little amount of bits likewise the required substance of data isn't lost inside the real picture. Represented least number of bits by utilizing image pressure. At the point when image are exchanged over the network it requires space for capacity and time to transmit image Huffman coding gives better image quality than image compression. This system is useful mobile authentication whenever you are going to logging secure channel for example mobile payment system etc.

Key words: Data Authentication, Data Compression, Visual Encryption, Huffman Coding

I. INTRODUCTION

Today is technical day each and every things are available on internet and each and every person are using system so authentication is needed. Area of Visual Cryptography is winding up being principal in the present range in which data security is of most extraordinary concern. Security is a basic part of Digital world. Cryptography is of two types first basic cryptography it's perform on content and another is VC performs on visual information which is picture furthermore, content. Cryptography is the examination of private information whether conferred over secured or unsecured channel from unapproved access, of ensuring data grouping, dependability and approval, and extraordinary end eavours. Cryptography contains two phases' encryption and decryption. Sender scrambles (change over plain substance into figure message) the message using the secret key also, later sends it to the recipient. Encryption is the path toward changing the picture into some other picture using an estimation with the goal that any unapproved individual cannot recollect it. Visual cryptography is connected up to riddle sharing. Visual puzzle sharing scramble a secret picture into clear parts which are called as offers with the ultimate objective that stacking a satisfactory number of offers reveals the riddle picture. Another terminology is image compression because if we are sending data with image on network then needed to less bit of data due fastest growth. Image compression is a sort of an application for information/picture pressure in which the essential picture gets encoded with the restricted bits. To lower the irrelevance and the redundancy of image data is the major target of the image compression is to enable them to get saved or transmit the data in the better form. Image compression is the lowering of the image data size, additionally with keeping up the required points of interest. Compression methods are developed quickly to pack colossal records of data like pictures. By the fast development of the innovation a huge amount of picture information ought to be figured out how to store those pictures in the best possible way by the utilization of powerful systems ordinarily brings about the compacting pictures. The compress image is the significant focus of this paper by diminishing the quantity of the bits based on per pixel which is expected to indicate it and furthermore to bring down the season of transmission for the transmission of pictures and for remaking again by the Huffman encoding calculation.

In this authentication system face image with information is split into two share using visual cryptography. First share is store in server database and second share is store where authentication is needed. During the authentication user firstly download first share and match second share if share are correct then you are able to right person.

II. IMAGE

An image is a 2-D signal that is processed by human visual systems [1]. These signs that are speaking to a picture are normally as analog. Although for the capacity, preparing and the transmission through the PC applications, these signs should have been changed over from the simple frame to their advanced shape. An Image or an advanced picture is typically a 2-Dimensional exhibit of the pixels. In the crude shape, the pictures may cover a tremendous measure of the memory in the RAM and in the capacity, both. Picture pressure is for decreasing the excess and unimportance of picture/information to enable them to either store or transmit the information better way.

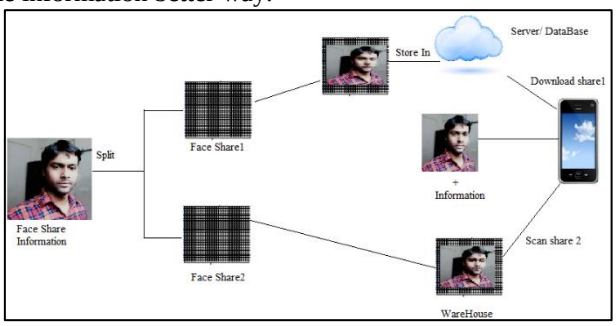


Fig. 1:

III. RELATED WORK

In huge technology in security in recent year, there is a numerous success in term of performance. There are lot of intelligent algorithm that are allocating to secure communication. Based on application they are different type are classified into spatial domain technique and frequency domain technique. The cbasic of Visual Cryptography was first proposed by Naor and Shamir[2]. Generally visual

cryptography takes place an image where image is split into two share. Share1 and share2. VC encrypts a secret message message into n offers to be disseminated to n members. Each offer shows commotion like irregular highly contrasting examples and does not uncover any data of the mystery picture independent from anyone else. Visual cryptography is very similar to one time pad. Divya James and Mintu Philips proposed a method to detect phishing websites using VCS [3]. In this author talk about user select random number during registration phase. Server generate random number of captcha and encrypt two share using visual cryptography. The number generate captcha can treated as password. S.k hifzul [4] 2015 has provided three party secret word Passwords such as that user cannot memorize complicated password which is easy to recognize.[5-7].

A client enrolment is support strong passwords for safeguard to remember and protection. The client enrolment process permits choosing while influencing users proposed for difficult passwords. The task of selecting weak passwords is more monotonous, avoids users from making like choice. This kind of enrolment plans it is use for exceptionally ensured secret key. Instead of increasing the burden on users, it is much easier to use the system's proposals for a secure secret key a component missing in many plans. The earliest approach in the category of draw metric systems constitutes draw-a-secret (DAS) [8]. The essential tide of DAS is to disentangle the issue of contrasting representations by encoding the he freehand drawing into a distinct code of symbols. This specific transformation from a sketch to a code is done by methods for a somewhat coarse technique. A prominent example of a possession-based authentication system is Pico [9]. It sends an individual handheld token that holds the clients qualifications and is opened through computerized adornments worn by the proprietor. The Pico confirmation convention is in light of an open key.

IV. SECURITY ISSUES IN WIRELESS NETWORK

Wireless network is emerging field of computer science as well as communication technology that you connect each and every device through network in wired less. Now a days are technological days where each and every person want to communicate because its simplicity robustness and 24*7 availability. So security is main concern now a days that how to manage and secure system from intruder. Over a decade there have been massive changes to way of communication of people. Like in vintage people are communicate through handshaking mailing etc. but recently devices are changes from pc to communication system like mobile phone PDA etc. that devices are connect wireless .

There are some point to consider security parameter that can create issue.

– Violation confidentiality

Confidentiality means there is no other person between site A and site B. means site a and site b can communicate to each other no other person can interrupt but violation of confidentiality is main issue.

– Access control

Access control is a type of limitation constraint that who is utilize the system. It is technique that control the unauthorized access. But violation of access control is issue of wireless network that some try to violate the access control.

– Authentication

It is parameter that communication are one system to another system is genuine. But there is issue that violation.

– Integrity

Integrity mean data that are sending to one person to another person that are reaching to same. But security issue is that some on try to changes.

A. There Are Some Attack

Attack can be two types that External attack and internal attack. Let's us see the definition if these parameter.

1) External Attack

External attack can be active attack and passive attack. Active attack are those attack that intruder try to change the data. Passive attack are those attack that intruder try to read and monitoring data.

2) Internal Attack

An internal attack may arise that when internal person of organization can try to destroy organizational assets.

B. Denial of Service Attack

DOS attack is a type of cyber-attack where hacker seek to make a machine unavailable to its legitimate user temporarily disrupting services of host connected to the internet. It means that if you are using website then attacker try to increase traffic to website that legitimate user cannot understand what's going on. So user cannot use the particular website this is knows as dos attack. That is main issue of network security.

C. Social Engineering

This is another types of issues of wireless network. Social engineering is a way form attacker try to access is network .By exploiting the trusted nature of your employee. It is art of science of getting people to comply with your wishes.

1) Downloading Malicious Content

This is another types of security issues because on internet lots of content are available some are good some are harmful. So downloading is other issue that what type's data you are download.

2) Illegal Activities

Illegal activates is type of issue because what are you searching and typing that are recorded. If you are going to wrong way that harmful for you.

V. PROPOSED SYSTEM

In this system we proposed visual cryptography and Huffman coding for encryption and data compression.

A. Visual Cryptography

One of most important technique for providing authentication, It is a science sending and receiving encrypted message that only decrypted by receiver or sender. Encryption and decryption is generally done by mathematical operation or algorithm.in a way intruder is not recipient and not read the message. Naor and Shamir[10] introduce visual cryptography scheme. It is secret sharing scheme that require less computation and decryption by human visual system. In visual cryptography scheme original image are divided into n share of scheme and each and every share printed in separate

transparency and decryption is performed by imposing the share. If all k share imposed, original image will reveal. In this visual cryptography each pixel of image contain a block. The block having equal

Number of white and black block. If pixel is divide into two part then one part is white and another is black. If pixel is divided four block part then then two white block and two black block. In this visual cryptography scheme is a secret sharing scheme that require less computation and decryption by human visual system. In this visual cryptography I use (2, 2) visual cryptography scheme. In (2, 2) visual cryptography original image are divided two share.

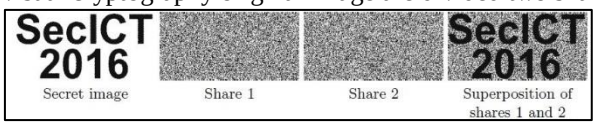


Fig. 1:

B. 2 Out Of 2 Visual Cryptography

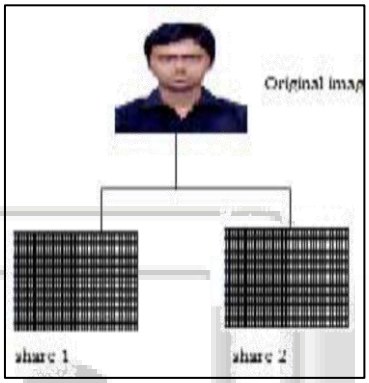


Fig. 2

In this schema white and black pixel is expand two sub pixel by randomly as shown in figure. For black pixel we get result but for white pixel we get result for gray because 50% contrast is lost in white pixel in encryption process.

Pixel	White		Black	
Probability	Way1 50%	Way2 50%	Way1 50%	Way2 50%
Share1				
Share2				
Share1+Share2				

Fig. 3:

C. Huffman Coding

In software engineering and data hypothesis, a Huffman code is a specific sort of ideal prefix code that is regularly utilized for lossless information pressure. The general thought in the Huffman encoding calculation is to distribute the plain short code-words to those squares of contribution alongside the high potential outcomes and the long code-words are designated to those which are having the low probabilities.

The Huffman code process is dependent on the two observations mentioned below.

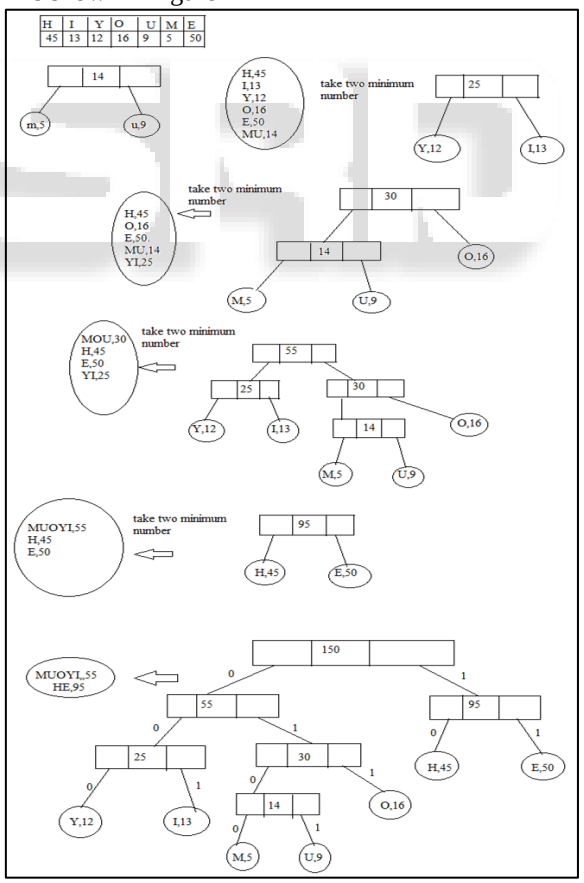
a) Frequently discovered images will have the shorter code-words as contrast with the image which discovered less much of the time.
b) Two symbols which found least frequently may have the equal length.

The Huffman code is set up by joining together two least conceivable characters and that are rehashing in this procedure to the extent there is just the one character is remaining. A code-tree is thus arranged and after that a Huffman code is created from the labelling of code tree. It is the best prefix code that is produced from the arrangement of the probabilities and which has been utilized in the diverse uses of the pressure. These generated codes are of different length of code which is using integral number of the bits. This idea brings about a decline in normal length of the code and consequently the entire size of the compacted information is turned out to be littler as contrast with the first one. The Huffman's calculation is the principal that gives the answer for the issue of building the codes with less excess.

D. Image Compression Benefits

a) It empowers a solid cost of investment funds that is incorporated with the sending of less information on the system of exchanged phone in which the cost of call is typically subject to its term.
b) It is not only to decrease the requirements of storage but also decrease the entire time of execution.
c) It eliminate chances of the errors transmission as
d) d). It empowers a level of the security against checking the unlawful Activities.

As shown in figure 4



VI. BENEFIT OF FACIAL AUTHENTICATION

A. No More Time Fraud

One of the huge advantages of utilizing facial biometric frameworks in your organization is that you won't need to stress over time extortion.

B. Better Security

You'll likewise appreciate better security with a face biometrics framework. Not exclusively would you be able to track workers through biometrics time participation following, yet any guests can be added to the framework and followed all through the region as well.

C. Easy Integration

Incorporated Biometric facial frameworks are additionally simple to program into your organizations PC framework.

D. High Success Rate

Facial biometrics innovation today has a high achievement rate.

VII. RESULT & DISCUSSION

In this paper we use .net technology. Whole result are Written in c# language as front end and Microsoft SQL Server 2008 are used in backend. By working of image authentication following original image result has been computed and improvement image quality. AS shown in figure 5.

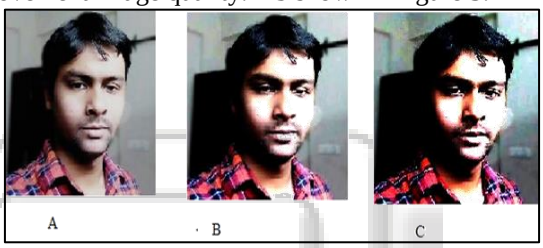


Fig. 5: Image Enhancement Transform

A. Poor Password That Leads To Attack

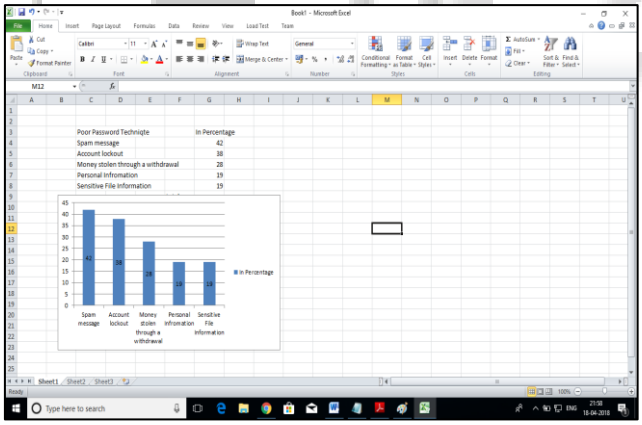


Fig. 6: Survey Done By 1000 U.S People That Are Reuse Password

These survey are done by 1000 us people that are majority of American reuse password

- 42% spam password sent from account.
- 38% locked account.
- 28% money stolen from bank through unauthorized purchase.
- 19% Personal information stolen like dob etc.
- 19% sensitive file etc stolen
- These data collected by Irvine, Calif. – July 19, 2017 – SecureAuth Corp[11].

VIII. CONCLUSION

Visual Cryptography is a new developments are making this stream all the more consolidating. It is the most secured concept attributable to scrambled offers at various levels utilizing the keys without which one can never unscramble the picture. This authentication is based on whenever user want to access secure channel like mobile payment system. In this payment system need to higher login system so face authentication provide security against user name password. In this user firstly need to download first share and match second share when share are match then you are access secure channel.

REFERENCES

[1] JayavrindaVrindavanam ,SaravananChandran, Gautam K. Mahanti, "A Survey of Image Compression Methods" International Journal of Computer Applications 2012.
[2] M. Naor and A. Shamir, Visual cryptography, in: Advances in Cryptology (Eurprocrypt94), Lecture Notes in Computer Science, vol. 950, Springer, Berlin, 1995, pp. 1-12.
[3] Divya James, Mintu Philip, A Novel Anti Phishing framework based on Visual cryptography in International Journal of Distributed and Parallel Systems Vol.3, No.1, January 2012, pp. 207-218.
[4] S.H., 2015. Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps.
[5] S. Chiasson, R. Biddle, and P. van O orschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc.ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
[6] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
[7] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Bddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security , Nov. 2009.
[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, USA, 1999, p. 1.
[9] j. Roth, X. Liu, and D. Metaxas, "On continuous user authentication via typing behavior," IEEE Trans. Image Process., vol. 23, no. 10, pp. 4611–4624, Oct. 2014.
[10] M. Naor and A. Shamir, Visual cryptography, in: Advances in Cryptology (Eurprocrypt94), Lecture Notes in Computer Science, vol. 950, Springer, Berlin, 1995, pp. 1-10.
[11] https://www.secureauth.com/company/newsroom/secureauth-survey-majority-reuse-

