Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/45

Visual Cryptography Authentication for Locker Systems using Biometric Input

Prabhdeep Singh[1], Dibyahash Bordoloi[2]

[1]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[2]Department of Computer Science & Engineering,Graphic Era Hill University, Dehradun, Uttarakhand India, 248002

ABSTRACT

Visual Cryptography is an encryption method that uses visuals to conceal data that can then be decoded visually with the right "key" image. In this method, a hidden picture is split into many "shares," each of which is divided into smaller "parts" based on the variance of its pixels. Identity may be confirmed automatically using a person's unique physiological or behavioural features; this is the field of study known as biometrics.

An encrypted and biometrically authenticated locker system is the goal of this project. In order to produce shares that will be divided between the admin database and the user, the fingerprint image of the user is treated as a secret image. The user's identity will be verified by comparing their live fingerprint scan to a synthetic fingerprint created by combining their shares.

Keywords: Visual Cryptography, live fingerprint.

INTRODUCTION

Security for Images : Using a method called "visual cryptography," a picture may be split up into separate sections that no unauthorised viewer would be able to decipher. Pixel expansion, contrast, security, accuracy, computational complexity, share created (meaningful or meaningless), and the nature of the secret picture are all factors that affect the performance of a visual cryptography method. Using this method, the original picture is encrypted into a set of shares that, when stacked, disclose the original image[1,2].

The Visual Cryptography Scheme is a method of cryptography that encrypts visual data in a way that makes decryption possible via the use of the human visual system[3]. You may do this with any of the following access structure plans: Threshold voltage control system

The hidden picture is revealed when two encrypted shares are superimposed; this is the simplest threshold approach for doing so. The creation of such an access structure does not need any extra data.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/45

Threshold VCS (2, n) scheme
Using this method, the secret picture is split into n pieces, each of which is encrypted in such a way that the secret image may be decoded by superimposing any two of the pieces.

Threshold VCS scheme (n, n)
This method divides the secret picture into n separate pieces, each of which contains a little piece of the hidden picture.

Threshold VCS scheme (k, n)
This method uses encryption to split the secret picture into n pieces that, when combined in groups of at least k, expose the original image.

Authentication Using Biometric Measures
To provide safe access to computers and other electronic systems, biometric authentication makes use of an individual's distinct biological traits. Fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keyboard dynamics, DNA, and signatures are all examples of biometric identifiers that may be used in conjunction with one another to reliably identify a person. To validate a user's identify and provide them access to a system, biometric authentication makes use of that evidence of identity[4]. Current biometric data is compared to historical data saved in a database. If the biometric data from the two samples are a perfect match, then the authentication is successful and the user is permitted access.

Iris identification uses the unique patterns in the ring-shaped area around the pupil of the eye to identify a person. Retinal scanning creates a picture of the blood vessel pattern in the light-sensitive surface of the inner eye.

Facial recognition systems use numeric codes called face prints, which identify 80 nodal points on a human face; voice identification systems rely on characteristics created by the speaker's shape of the speaker's mouth; and finger scanning, the digital version of the ink-and-paper fingerprinting process, uses details in the pattern of raised areas and branches in a human finger image.

LITERATURE SURVEY

How Visual Cryptography Works
Each hidden picture is partitioned into shares in accordance with the VC scheme used. Even while each individual sharing seems to be completely random and provide no clues as to the hidden picture behind it, when stacked up they reveal the image [5].

Distinct Visual Encryption Methods
For the purpose of implementing Visual Cryptography in photographs, a number of different approaches have been suggested.

An Arrangement for Visually Distributing Confidential Information (VSSS)
A binary image (picture or text) is converted into n transparencies of random pictures using this k-out-of-n VSSS or (k,n) technique. When any k out of n sheets of the transparency are combined, the

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/45

original picture is shown, but less than k sheets cannot. Using a VC system where 2 out of 2 outcomes are favourable [6]

A 2 out of 2 VC system. In this case, the theory of colour blending is put into practise. When two transparent sheets of different colours are stacked, the result is a new, hybrid hue. Extending the Capabilities of Visual Cryptography

To better capture the beauty of natural scenes, devised a VC system. It's the process that gives binary shares their actual value. It shows a system that, given three photographs as input, can produce two images that are near-perfect matches for two of the original images. Reconstructing the third image requires printing the first two onto transparencies and stacking them.

Protocol for Binary Image Encryption

Using grayscale pictures with the binary visual cryptography technique. In accordance with this, the grayscale picture is converted to a halftone image, and then two visual cryptography transparencies are made. These portions are created using halftone techniques and colour decomposition[7]. After breaking the colour picture into its component halftones (yellow, magenta, and cyan), he used the subtractive colour model to create three different 2-out-of-2 VC schemes. Visual ciphering based on halftones

Halftone visual cryptography in 2006, and their results are of great quality and meaning. The visual information is included in the created halftone shares. Each of the "n" shares of halftone visual cryptography has an array of Q1 x Q2 ("m" in basic model) subpixels, called halftone cells, that encode a secret binary pixel "P." Schemes for Visual Cryptography and Their Comparison

A SECRET IMAGE-SHARING SYSTEM BASED ON A 2OUTOF2 SYSTEM

The 2-out-of-2 approach divides the picture's secret pixels into two parts and then recovers the original image by adding the two parts together. Using this method is the same as doing an OR or XOR operation on the stocks[8].

Algorithm for a 2-out-of-2 secret-sharing scheme (2-out-of-2 VC Share Generation Algorithm)
Input: a covert two-dimensional picture
Results: 2 pointless stock shares S1 and S2

1) Determine the dimensions of the hidden picture.
2) IMG WIDTH=2, IMG HEIGHT=3, then 4: Get the initial fraction S1 of width*height as a binary random matrix, S1=Random matrix.
3) Bitwise XOR the first share with the secret picture to get the second share S2 of width * height.
4) Send Back S1, S2
5) Exit.
6) Existing System
7) Lockers with Keys

Manual locks are standard in most residential and commercial lockers as well as safe deposit

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/45

boxes. A manual key is required to open the locker. Accessing or replicating these is not too difficult. Anybody can go into the locker with no problems since there is no additional kind of identification or authentication required.

Systems for Digital Lockers

There is no need for a key when using a digital locker system since each locker is equipped with a digital lock. A little screen is installed on the locker for this digital system. A computerised system linked to an integrated controller handles locking and unlocking of lockers in homes and hotels by checking the user-set password. Lockers that Use Global Positioning System Technology [9]

A digital system built into each locker is linked to a central server housing a user database. The digital system generates a random number that is specific to the user by using different personal characteristics of the user, such as the date of birth and the user's ATM pin and the date of the particular day. The locker's screen will show you this random number. To get access to the locker, a user must first look at the random number and then text that number to the admin computer using the cellphone number they used to register for the locker. GSM technology is used for the transport of messages. Storage Space using RFID-Based Lockers

An RFID reader, GSM modem, keyboard, and LCD make up this system. In order to communicate with the microcontroller, the RFID reader must first get the id number from the passive tag. If the ID number is correct, the microcontroller will send a text message (SMS) to the verified user's mobile phone, asking for the original locker access code. The microcontroller will compare the password typed on the keyboard with the one sent from the authorised cell phone [10]. When these two codes are a match, the safe will unlock. Safes with Biometric Identifiers for Access Control

Locking and unlocking the lockers in these systems is accomplished by fingerprint recognition or other biometric criteria, such as a retina scan. A user's fingerprint is recorded by the system. only the authorised user is able to unlock the locker and take its contents by requiring a fingerprint match to reopen the locker door. Customers will like not having to remember to bring the key, and the added sense of security they'll get from using this approach. A DigiLocker is a secure online repository for electronic documents and the Uniform Resource Identifier (URI) links to those documents provided by different issuer departments. DigiLocker's e-Sign feature allows users to digitally sign electronic documents.

THE SUGGESTIVE SYSTEM

The suggested locker authentication system features a two-stage procedure:

• Registration \s• Login \s Registration

The system detects a valid user by scanning his or her fingerprint. Using visual cryptography methods, the fingerprint picture is segmented into pieces. Both the system database and the user have a copy of the data, but the system keeps one. A proper table is created in the database after the share is linked to the user id. In this table, the user id will serve as an index to all of the shares that are associated with that user id.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/45

Login Block Diagram

Registered users may access their lockers by entering their user id and the share that has been saved with them. This user id will be compared to the stored user id in the system. When a user's fingerprint is successfully matched with one in the database, the two halves are joined to generate a whole fingerprint picture. In addition, the user's fingerprint will be scanned in real time and compared to a fingerprint picture produced from the user's shares. The user is authenticated and granted access to the locker only if the two fingerprint pictures match in real time. Lockers may be locked and unlocked from either side thanks to this method. Because each person's fingerprints are completely unique, the visual cryptography sharing method may be used to guarantee that no unauthorised person will be able to gain entry to the safe.

APPLICATIONS

Cassette for storing ammo in the military The suggested method may be used to secure military ammo boxes, which are used to transport or store weapons and ammunition, from unauthorised individuals. A hacker will have a hard time penetrating the suggested two-tiered protection mechanism. Keeping records digitally

Documents, PDFs, pictures, photographs, and more may all be kept safely and securely online with this system. In this approach, an easy authentication method may be used to keep any digital file safe. Safety deposit boxes and jewellery vaults

Large sums of money are stored in cash and valuables in bank lockers. Using the suggested technology, the bank's valuables and cash may be kept safe while only authorised personnel and customers can access them for transactions. Private and public safes

Valuables such as jewellery, cash, and sensitive documents may be safely stored in a home safe deposit box. Using this method, you can be certain that these crucial facilities are being stored securely.

CONCLUSION

The field of visual cryptography is ripe for exploration at the moment. The traditional visual cryptography paradigm has been extended in several novel ways. The current Locker Systems save the user's password in the system database. In contrast, the suggested system relies on the user to provide the password in real time, with the database initially holding just half of the shares, which is of little utility on its own. Therefore, the suggested system offers two layers of security by encrypting and exchanging fingerprint images and using biometric fingerprint authentication to verify the identity of each user.

Using the suggested authentication method, secure electronic lockers for keeping the sensitive electronic documents may be created. Improve the project by including other biometric characteristics, such as retinal and iris patterns, voice structure, hand and ear morphology, and so on. Combining two or more biometric features for authentication is possible.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/45

REFERENCES

1. Wang, Y. R., Lin, W. H., & Yang, L. (2013, July). A lossless watermarking using visual cryptography authentication. In 2013 International Conference on Machine Learning and Cybernetics (Vol. 3, pp. 1109-1113). IEEE.
2. Chavan, P. V., Atique, M., & Malik, L. (2014, March). Signature based authentication using contrast enhanced hierarchical visual cryptography. In 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science (pp. 1-5). IEEE.
3. Altaf, A., Sirhindi, R., & Ahmed, A. (2008, August). A novel approach against DoS attacks in WiMAX authentication using visual cryptography. In 2008 Second International Conference on Emerging Security Information, Systems and Technologies (pp. 238-242). IEEE.
4. Dalvi, G. D., & Wakde, D. G. (2017, April). Facial images authentication in visual cryptography using sterilization algorithm. In 2017 2nd International Conference for Convergence in Technology (I2CT) (pp. 951-955). IEEE.
5. Mathivadhani, D., & Meena, C. (2010, December). Digital watermarking and information hiding using wavelets, SLSB and Visual cryptography method. In 2010 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-4). IEEE.
6. Nandhinipreetha, A., & Radha, N. (2016, January). Multimodal biometric template authentication of finger vein and signature using visual cryptography. In 2016 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE.
7. Suryadevara, S., Naaz, R., Kapoor, S., & Sharma, A. (2011, September). Visual cryptography improvises the security of tongue as a biometric in banking system. In 2011 2nd international conference on computer and communication technology (ICCCT-2011) (pp. 412-415). IEEE.
8. Wang, G., Liu, F., & Yan, W. Q. (2016). Basic visual cryptography using braille. International Journal of Digital Crime and Forensics (IJDCF), 8(3), 85-93.
9. Vyas, C., & Lunagaria, M. (2014, December). A review on methods for image authentication and visual cryptography in digital image watermarking. In 2014 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-6). IEEE.
10. Luo, H., Pan, J. S., Lu, Z. M., & Liao, B. Y. (2007, October). Watermarking-based transparency authentication in visual cryptography. In Seventh international conference on intelligent systems design and applications (ISDA 2007) (pp. 609-616). IEEE.APA