International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7058
Article Received: 20 March 2023 Revised: 30 April 2023 Accepted: 15 May 2023

Sharing Secret Colour Images with Embedded Visual Cryptography Using the Stamping Algorithm and OTP Procedure

Nilesh N. Thorat[1], Dr. Amit Singla[2], Dr. Tanaji Dhaigude[3]
[1]Research Scholar, Computer Science and Engineering ,
Nirwan University, Jaipur, India
nileshthorat4694@gmail.com
[2]Research Guide, Professor, Computer Science and Engineering ,
Nirwan University, Jaipur, India
amitsingla70@yahoo.com
[3]Research CO-Guide,CSE Department, Fabtech College of Engineering and Research, Sangola, MH.
tanajidhaigude@gmail.com

Abstract- Finding a way to ensure the safety of media is becoming increasingly common in the modern world as digital media usage increases. Visual cryptography (VC) offers an efficient method for sending images securely. Images that have been protected using visual encryption can be decoded using features of human vision. Emails are not a highly safe method of exchanging private data because someone else can quickly weaken the content. In the visual cryptography technique, we presented for colour pictures, the divided shares are enclosed in additional pictures using stamping. Using a random number generator, the shares are created. Visual cryptography schemes (VCS) are a method of encoding pictures that conceals the secret information which is present in images. A secret image is encrypted using a straightforward visual cryptography technique by splitting it into n shares, and the stamping operation is carried out by overlapping k shares. It can be beneficial for hiding a secret image. There is a chance that employing cryptography for information exchange could cause security problems because the process of decryption of simple visual cryptographic algorithms can be completed by the human eye. To address this issue, we are using the OTP procedure. In the past, static ID and passwords were employed, making them susceptible to replay and eavesdropping attacks. One Time Password technology, which generates a unique password each time, is utilized to solve this issue. The suggested approach strengthens the security of the created transparencies by applying an envelope to each share and employing a stamping technique to address security vulnerabilities that the previous methods had, such as pixel expansion and noise.

Index Terms- Visual Cryptography schemes, Encryption and Decryption, One-Time-Password, shares. Stamping algorithm.

I. INTRODUCTION

Transferring multimedia material via the World Wide Web is now instead usual. There is a pressing need to find a solution to the issue of assuring information safety in today's increasingly open network environment with the advent of the electronic commerce age. Multimedia content is simply transmitted over the Internet thanks to the quick development of network technology. The Internet is used to communicate a variety of sensitive information, including commercial identifications and military maps. Security concerns must be taken into consideration while using confidential images because to gain data, attackers can take advantage of communications networks' weak points. Several picture confidential sharing systems were generated to address the security issues with secret photos. [1]

In 1994, Naor and Shamir established the concept of visual encryption. If the right important pictures are utilized, visual cryptography, a type of encrypted that hides data within pictures, is able to recover by the eye of a person.VC is the idea of splitting an encrypted image into "n" parts and then overlaying a specific subset of those "n" shares to expose the image that is hidden. Obtaining the data via one of the shares is challenging. The information must be disclosed with an acceptable amount of transparent shares. Stamping the two layers onto a clear sheet is the most straightforward way to put this plan into practice.

In the case of the VCS, a picture or piece of information is provided as an input in the form of an image, and the system creates "n" (2n) parts that resemble pictures of random disturbances. To expose the secret image, the user must load "k" number of parts, where 2kn is the number of shares. The

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7058
Article Received: 20 March 2023 Revised: 30 April 2023 Accepted: 15 May 2023

primary benefit of this method is that the secret image may be deciphered by the human visual system without the need for any complicated calculations. The confidential picture can be hidden in n different images, or shares, according to Naor and Shamir's plan. The hidden image can then be easily revealed by loading up to k of the shares together. Each sharing appears to be a collection of random pixels. Before being added to the others, a single share often has no information about the hidden image. If the secret is binary, shares can be meaningful by applying the stamping procedure in Ref. But because there are so many random pixels in the colour secret image, the shared information is only partially relevant. Therefore, in the suggested approach, a cover picture is stamped to the random share without using a physical watermark. The cover pictures were colourful pictures with 24 bits (8 bits in each plane) of representation. The shares that appear arbitrary are denoted by 8 bits. The suggested method incorporates these eight bits of a pixel electronically into the cover image's 24-bit pixel.

The Little Substantial Bits for every layer of the cover picture can be changed to accomplish this. Because basic visual cryptographic systems can be decoded by the human eye, there is a chance that employing cryptography for exchange of data will cause security problems. To address this issue, we have chosen the One-Time Password (OTP) method. A randomized password is created by a special algorithm known as a one-time password generator each time. It functions as a device or algorithm that receives user input and generates a new password that is distinct from passwords that have already been produced. The safety of networks focuses on identifying users using a username and password, however because this method is prone to numerous attacks, every time a new password is used for verification, regardless of whether the old password was lost or stolen. The primary component of an individual password structure, which generates random passwords, is a one-time password generator. Server and client identification are other components of the system.

The one-time password is safe since

1. it can't be utilized more than once

2 cannot be reversed to get back to the source.

It primarily addresses the two components.

1. The Key;

2. A Counter

One password is generated at a time by an OTP system and given to the user for verification. OTP sends the clients via text messages or email.

II. EXISTING SYSTEM

Varsha Himthani et. al.2022, suggested this method, the plain image is converted to a picture that is encrypted using a private key and an algorithm for encryption. The encrypted image appears chaotic and is therefore likely to catch the attacker's eye. Important data may be exposed if an image is taken and layered. The Visually Meaningful Encrypted Image (VMEI) technology, which first encodes the original picture then hides it in a reference image, has been created in this regard. The finished encrypted image resembles a typical image. As a result, the VMEI methodology offers greater security than straightforward picture encryption methods. As a result, this work presents a rigorous survey of current VMEI approaches. According to their traits, the VMEI approaches are categorized into many groups. [1]

K Alghathbar et. al.2021, suggested this method The implementation of dual-factor authentication utilizing SMS OTP, or One Time Password to Secure a Transaction (SET), is discussed in this work. The suggested strategy ensures authorized operations in services like internet banking, e-commerce, or ATMs. The suggested approach comprises creating and sending a One Time Password (OTP) via SMS (Simple Message Service) to a mobile device. The produced unique password is created and confirmed utilizing a Secure Cryptographic Algorithm, and it is only valid for a brief amount of time that the user defines. The suggested technique has been utilized effectively and verified. [2]

K Anish; C K Sai Dinesh; S Ranjit; E Venkatesh; S V Shruthi. et. al.2022 This study presents a method for digital image watermarking and k-n sharing. In order to watermark digital images, tools like the wavelet transform and cosine transform are used. The watermarks would be used to validate an image when it was the input signal. The system is impervious to several attacks and common image processing operations. In the case of KN Secret Sharing, an input picture is encrypted using a user-supplied key. The picture being provided has been further divided in N independent parts via the K out of N method. The end user only needs K of these N shares, even though they can be spread, to create the actual image. [3]

Jitendra Saturwar; D.N. Chaudhari et. Al. 2017 the present research examines different algorithms that generate sizable shares. All of these shares are watermarked with cover pictures. Following delivery of these watermarked images to the other end, the recipient will extract the meaningful shares from the watermarked images, stack them, and then create the original concealed image. Visual encryption and digital watermarks are used to more safely preserve secret images. [4]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7058
Article Received: 20 March 2023 Revised: 30 April 2023 Accepted: 15 May 2023

Suiang-Shyan Lee; Yi-Jheng Huang; Ja-Chen Lin et.al.2019 in this paper, the standard visual encryption methods are expanded to online pages. The crucial idea is that layering operations can be simulated by Collapsible Style Sheet mix modes. Each blend type can be compared to the exclusive-OR (XOR) operator, and the multiply blend mode to the Logical OR operators. [6] Thus, by simply overlapping shares, secrets can be discovered via a web browser without the need for further calculation. This plan was given the name Web-VC. Although electronic shares may be utilized in this instance, the method of decoding for Web-VC is the same as that for conventional visual cryptography. Without compromising its integrity, Web VC has a high capacity to withstand compressing and translation. This paper also offers the XOR-based flip cryptography visual technique. [5]

III. PROPOSED METHODOLOGY

Visual Cryptography: - Visual data (images, text, etc.) can be encrypted using a cryptographic method known as visual cryptography so that when the data is decoded, an image in visual form is produced. Moni Naor and Adi Shamir are given credit with creating one of the most well-known approaches in 1994. The advantage VCS encrypting process, where protected data is decoded using the Human Visual Systems (HVS) without requiring to use challenging mathematical algorithms. The k-n private sharing system is a special kind of visual cryptographic method in which only a portion of k shares out of n shares shows the confidential data, fewer of it will provide nothing, and while decoding the recipient must provide an identification code to decrypt the picture.

1.Encryption Process

It includes creating shares applying any fundamental visual encryption scheme. The formation of a (2, 2) VC share is carried out under the plan we've suggested. The secret image has 4 sub pixels for each pixel. Two identical sets of four sub pixels make up one white pixel. Two complimentary groups of four sub pixels make up one black pixel. Applying this method, the confidential image's pixels are all similarly encrypted. Shares come in three varieties: diagonally, horizontally, and vertically. Each single shared has even grey appearances since it is made up at randomly of 2 black and 2 white sub pixels. When two shares accumulate on top of one another, the result is either fully black (which depicts black) or medium grey (which represents white). The image-based confidentiality technique is predicated on the idea that each coloured pixel in the information is treated independently. For each transparency, n modified versions of each original pixel (referred to as shares) are present. Each part is made up of sub pixels produced close to one another so that the human visual system can average out every share's distinct features.

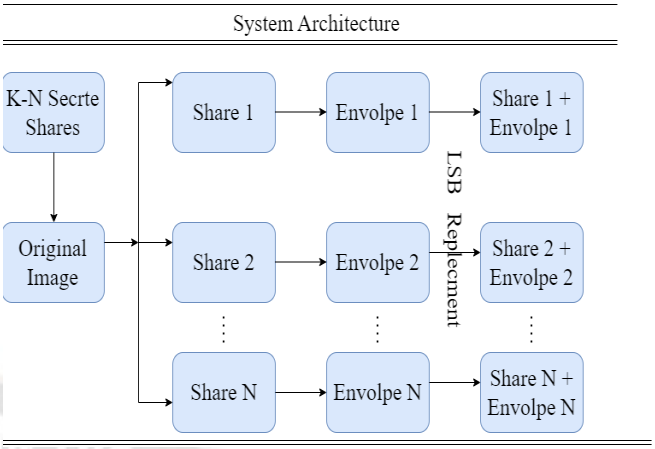

Figure No 1. System Architecture (Encryption Process)

2.Stamping Cover Images

The VCS generates spurious noise in the form of pieces. These kinds of arbitrary sharing, which can be hard for users to recognize, are of greater interest to attackers. The suggested strategy makes use of significant shares to overcome these obstacles. If a secret is binary, shares can be meaningful by applying the stamping procedure. But because there are so many arbitrary pixels in the colour secret picture, the shared information is barely relevant. Therefore, in the suggested approach, a cover picture is stamped to the randomized sharing without any pixel expansions using a digital watermarking method. The cover graphics are coloured pictures with 24 bits (8 bits in each plane), which are used for representing them.

A method known as the one-time password generating creates unique random passwords each time. It functions as a device or method that receives user input and generates a fresh password that is distinct from passwords that have already been produced. Security for networks focuses on users authenticating using their ID and password, however because this method is prone to numerous attacks, every time a fresh password is put in for verification, regardless of whether the old password was lost or stolen. The primary component of a one-time password system, which generates arbitrary passwords, is the one-time password producer. The client and the server verification are other components of the system. One password is generated at a time by the OTP mechanism and provided to the user for verification. OTP delivers credentials to users using SMS service, by telephone or by the written word. Login is secured by the software on user mobile is client verification and the server verification. One password is generated at a time by the OTP system and given to the user for verification.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7058
Article Received: 20 March 2023 Revised: 30 April 2023 Accepted: 15 May 2023

Overall Process

Step I:-Implementing a k-n secret sharing visual cryptography system, the original picture is split into n parts, where k parts are needed to reassemble the original image.

Step II: -Every one of the n shares created in Step I, are put in via LSB substitution into n distinct enveloped pictures.

Step III: - k encompassed pictures created in Step II are collected and the initial picture is rebuilt applying an OTP and LSB recovering by OR procedure.

4.Decryption Process: -

Cryptography Decryption is the procedure of restoring the decrypted version of information after encrypting has made it unreadable. In decryption, the system removes and changes the data into sentences and pictures that are simple to grasp for both the reader and the system. There are two ways for decoding data: personally and electronically. It can also be done using a set of keys that are regarded as input. The original image is obtained by performing an OR procedure on each of these pictures' last two bits of alpha, red, green, and blue (RGB) data for every pixel. According to this logic, a person's vision system functions like a binary OR operator. The scenario of stacked n enclosed pictures can be handled by the OR operator for created processes.

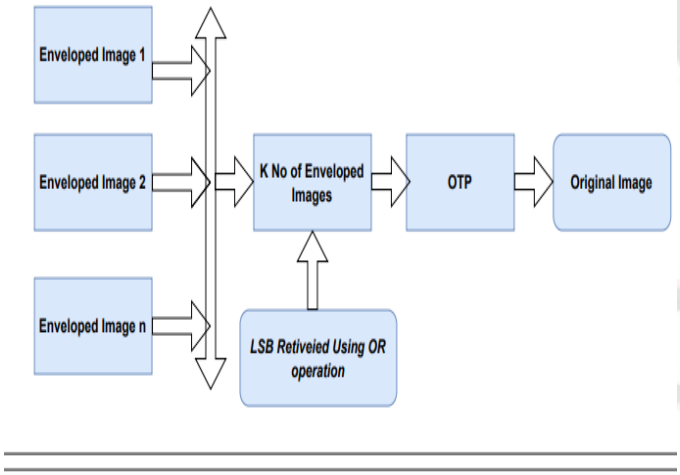

Figure No 2. Decryption Process.

3. OTP Process

A method known as the one-time password generator creates unique passwords that are random every single time. It functions as a device or method that takes input from the user and creates new passwords that are distinct from earlier generated passwords. Security of networks focuses on authentication of users using their ID and password, however this approach is prone to several attacks, therefore for reliable verification, a new password must be used each time, regardless of whether previous login was lost or hacked. The major component of a one-time password method is the one-time password system, which is used to create unique credentials. Client and server verification are other components of the overall system. Which depends on SHA-1, is a common OTP.The HASH methods utilized are MD4, MD5, although they are attackable. Another OTP depends on the Ping Pong-128 stream cipher, which produces integers that are random using the Ping Pong-128 method.

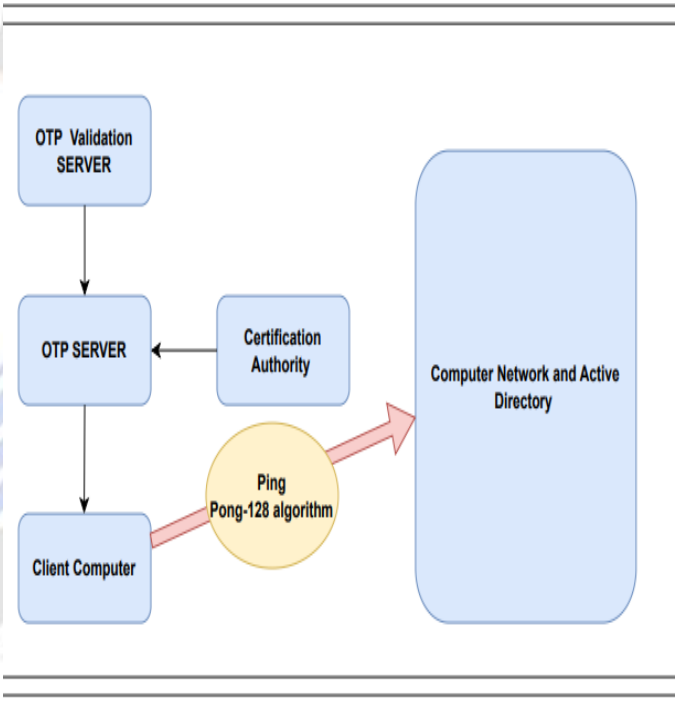

Figure No 2. OTP Process.

IV. ALGORITHMS

1. Algorithm for the k-n Secret Sharing Visual Cryptography Scheme: -

The input is an image. The user is also asked for input regarding the number of parts into which the image would be split (n) and the number of parts needed to rebuild the image (k). The algorithm used to divide is as follows.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7058
Article Received: 20 March 2023 Revised: 30 April 2023 Accepted: 15 May 2023

Step I: -
Take an image IMG as input and calculate its width(w) and height (h)
Step II: -
Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image where k must be less than or equal to n. Calculate RECONS = (n-k) +1.
Step III: -
Create a three dimensional array IMG_SHARE[n] [w*h] [32] to store the pixels of n number of shares. K-n secret sharing visual cryptographic division is done by the following process.

```
for i = 0 to (w*h-1)
{
      Scan each pixel value of IMG and convert it into 32 bit binary string let PIX_ST.
for j = 0 to 31
{
   if (PIX_ST.charAt(i) =1)
   {
   call Random_Place (n, RECONS)
    }
    for k = 0 to (RECONS−1)
  {
    Set IMG_SHARE [RAND[k]][i][j] = 1
  }}
```

Step IV: -
Create a one dimensional array IMG_CONS[n] to store constructed pixels of each n number of shares by the following process.

```
for k1 = 0 to (n-1)
{
  for k2 = 0 to (w*h-1)
  {
   String value= “” for k3 = 0 to 31
  {
   value = value+IMG_SHARE [k1][k2][k3]
  }
 Construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0. Construct pixel from these part and store it into IMG_CONS[k1] [4].
  }
  Generate image from IMG_CONS [k1]1 [8].
}
subroutine int Random_Place(n, RECONS)
{
Create an array RAND[RECONS] to store the generated random number.
for i = 0 to (recons-1)
} }
```

Algorithm 1: - k-n Secret.

2. Encryption Algorithm: -

The input taken an image. The client is also asked for inputs regarding the total number of parts into which the picture could be split (n) and the numbers of parts needed to rebuild the picture (k). The following method does the encryption, which is the split of the picture into n parts such that k parts are enough for reconstructing the picture.

Step: I: Take an image as input and calculate its width (w)and height (h).

Step II: Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image.k must be less than or equal to n.

Step III: Calculate recons=(n-k)+1.

Step IV: Create a three dimensional array img_share [n][w*h][32] to store the pixels of n number of shares.

Algorithm 2: - Encryption Algorithm

3. Using a random sequence algorithm, the original image is shared in secret. (k-N algorithm):-

Step I: The original image (Iw*h), number of shares to be divided (n) and number of shares needed (k) to retrieve the original image are taken as input.

Step II: The number of sequences (ns) of (n−k+1) number of „1"s and (k−1) numbers of 0"s i.e. nCk−1 is calculated. Subsequently the sequences Sq1, Sq2, .Sqns are constructed.

Step III: Let the shares of I denoted by S1, S2,..., Sn, each of size w X h. Shares are generated using the following logic.

i)Initialise all the bit positions of St by 0, for $1 \leq t \leq n$
ii) if (ith bit value of Ienc is 1)
{
Generate a random number „r" in the range 1 to n's. Perform OR between the ith bit of Sj share (where 1 j n) with the j Th bit of the sequence Sq , (1 r n's).
}

4. The processes for stamping (Shares and Covers) are proposed.

1. Keep going to each and every sharing.
2. Continue for each identical pixel.

Step 1:- Generate an array S[0…8] that contain the bits of a pixel value.

Step 2:- Decompose the colour cover into three components Red, Green, Blue and store bits of each component into three arrays R[0…8], G[0…8] and B[0…8] respectively.

Step 3:- Find that which channel contain more information, i.e which colour has less effect in the cover image.

Step 4:- Replace the 2 least significant bits of the rest two channel with the share pixel value and 4 least significant bits of the channel that have less effect.

Step 5:-. Stop .

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7058
Article Received: 20 March 2023 Revised: 30 April 2023 Accepted: 15 May 2023

5. Decryption Algorithm: -

Inputs used in this phase include at least k numbers of enclosing photographs. To produce the original image, an OR technique is used to combine the final 2 bits of the alpha, red, green, and blue from each of the images for each pixel. The OR mechanism of the human visual system was previously mentioned. For generated by computer processes, the stacking of k out of n enclosed images can be accomplished using the OR operation. The method that follows is used to carry out the data encryption operation.

Step I:- Input the number of enveloped images to be taken (k); height (h) and width (w) of each image.

Step II:-Create a two dimensional array STORE[k][w*h*32] to store the pixel values of k number of enveloped images. Create a one dimensional array FINAL[(w/4)*h*32] to store the final pixel values of the image which will be produced by performing bit wise OR operation of the retrieved. LSB of each enveloped images.

Step III:-

```
for share_no = 0 to k-1
{
Take the name of the enveloped image to be taken and store the pixel values in
STORE [share_no][w*h*32] using the following loop.
for i = 0 to (w*h-1)
{
Scan each pixel value of the Enveloped image and
Convert it into 32 bit binary string let PIX.
for j = 0 to 31
{
STORE[share_no][i*32+j] = PIX.charAt(j)
}}}
```

Step IV:-

```
Take a marker M= −1. Using the following process the last two bits of alpha, red, green and
blue of
each pixel of each k number of enveloped images are OR ed to produce the pixels of the
original image.
for i = 0 to w*h
{
 Consider 8 integer values from C0 to C7 and set all of them to 0 for SH_NO = 0 to k-1
  {
 c0 = c0 | STORE [SH_NO] [i*32+6]; // | is bitwise OR c1 =c1 | STORE [SH_NO] [i*32+7];
 c2 = c2 | STORE [SH_NO] [i*32+14];
 c3 = c3 | STORE [SH_NO] [i*32+15];
 c4 = c4 | STORE [SH_NO] [i*32+22];
 c5 = c5 | STORE [SH_NO] [i*32+23];
 c6 = c6 | STORE [SH_NO] [i*32+30];
 c7 = c7 | STORE [SH_NO] [i*32+31];
   }
 FINAL [++M] =c0;
 FINAL [++M] = c1;
 FINAL [++M] = c2;
 FINAL [++M] = c3;
 FINAL [++M] = c4;
 FINAL [++M] = c5;
 FINAL [++M] = c6;
 FINAL [++M] = c7;
}
Create a one dimensional array IMG_CONS[ ] of size (w/4)*h to store constructed pixels.
Construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit sub-string
from FINAL[ ] starting from 0.Construct pixel from these part and store it into
IMG_CONS[(w/4)*h] Generate image from IMG_CONS[ ]
```

Step V:-Stop

6. OTP Algorithm: -

The produced OTP needs to be challenging for attackers to decipher, recover, or track as a way to protect the computer system. Thus, creating a safe OTP producing system is crucial. To create difficult login credentials, the OTP technique can leverage a variety of factors. Consumers seem ready to use simple criteria such personal phone number and a unique identifier for operations including authorizing telephone tiny payment This method uses a (k, n) threshold system, where any data regarding S can't be ascertained from shares with a value of k-1 or less. Participants hold shares derived from a secret S. S is able to be retrieved from shares of K or more. Here, we employ a quick (2, n) limit so that we can obtain S with only a XOR procedure. This was quickly and securely demonstrated. In this approach, we produce a random number and use XOR to divide the hidden information into four equal pieces. After that, we encode and send the individual's one share through Text SMS. Assuming he is a legitimate user, he will confirm his approval of the deal by entering the OTP. Following decryption, that share gets compared to another share that is kept in the database. In order to produce a Secured and Random OTP, the Thresholds Secret Sharing Scheme (TSSS) is helpful.

1. To authenticate a user, servers ask for their email ID and password at login.

2. The server merely encrypts the user name and password before sending the output to the OTP generator.

3. The OTP producer begins to operate. OTP chooses two alphabets using an algorithm created from encrypted data.

4. Assuming it is a random key, we use genetic algorithms to generate a random 8 alphabets from those two alphabets.

5. We must choose 8 alphabets from the encrypted result and use them as the ID.

6. There are now two keys with eight alphabets. A random key is one, while a personal ID is another.

7. Split the random password and identifying ID into two groups of four alphabets each. I.e., IDL = Y1Y2Y3Y4 IDR = Y5Y6Y7Y8 where pswdL = X1X2X3X4 and pswdR = X5X6X7X8.

8. Generate an arbitrary point from an elliptic curve that satisfies the curve's elliptic model into an 8-bit binary format.

9. Complete the procedures in accordance with the binary value. Perform KL = pswdL (OR procedure) IDL KR = pswdR (OR procedure) IDR if b[i] == 0. If b[i] ==1, then execute KL = pswdL (OR procedure) otherwise. KR = pswdR

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7058
Article Received: 20 March 2023 Revised: 30 April 2023 Accepted: 15 May 2023

in IDL (OR procedure) F (IDR) F (IDR) is the product of the IDR and any random point on the elliptic curve, where.

10. KL plus KR added together equals K.

11. Combine IDL = ID and F (IDR).

12. Use any secret key to locate the ID product.

13. We currently maintain 8 random passwords and a newly created identification number (ID) in our database.

14. The subsequent time the user logs in; the OTP producer receives the ID to create the password.

V. CONCLUSION.

In the present study, an enveloping approach is developed employing the well-known k-n secret sharing visual cryptography technology, wherein the confidential shares are encased within blatantly innocent digital picture covers via LSB replacement. As it deceives the hacker's eye, this protects visual cryptography schemes from unauthorized attack. Simple visual cryptography relies on the human vision system for its decryption process, therefore if a person is skilled in k numbers of shares; the image can be simply deciphered using OTP. An effective method for providing users with random passwords is the one-time password. Since OTP generates a fresh username and password for every session, users aren't concerned if they forget their previous password. OTP shield identities of users from tracking or replaying attacks. Applying a generator of random numbers, a picture is divided into the number n of pieces.

REFERENCE

[1] Varsha Himthani; Vijaypal Singh Dhaka; Manjit Kaur "Systematic Survey on Visually Meaningful Image Encryption Techniques", 31 August 2022, IEEE.

[2] Dhabliya, P. D. . (2020). Multispectral Image Analysis Using Feature Extraction with Classification for Agricultural Crop Cultivation Based On 4G Wireless IOT Networks. Research Journal of Computer Systems and Engineering, 1(1), 01–05. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/10

[3] K Alghathbar "OTP-Based Two-Factor Authentication Using Mobile Phones", 11-13 April 2021, IEEE.

[4] K Anish; C K Sai Dinesh; S Ranjit; E Venkatesh; S V Shruthi "Performance Analysis of Visual Cryptography and Watermarking Algorithms" 27-29 May 2022,IEEE.

[5] Jitendra Saturwar; D.N. Chaudhari "Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking", 22-24 February 2017,IEEE.

[6] Suiang-Shyan Lee; Yi-Jheng Huang; Ja-Chen Lin "WEB-VC: Visual Cryptography for Web Image", 22-25 September 2019, IEEE.

[7] Hsiang-Cheh Huang, Jiun Lin,Yuh-Yih Lu "Visual Secret Sharing for Copyright Protection and Authentication of Colour Images",2015 Third International Conference on Robot, Vision and Signal Processing.

[8] Prof. Rathod V U Raisoni: N. P. Sable, R. Sonkamble, V. U. Rathod, S. Shirke, J. Y. Deshmukh, and G. T. Chavan, "Web3 Chain Authentication and Authorization Security Standard (CAA)", IJRITCC, vol. 11, no. 5, pp. 70–76, May 2023.

[9] Prof. Rathod V U Raisoni: N. P. Sable, V. U. Rathod, R. Sable and G. R. Shinde, "The Secure E-Wallet Powered by Blockchain and Distributed Ledger Technology," 2022 IEEE Pune Section International Conference (PuneCon), Pune, India, 2022, pp. 1-5, doi: 10.1109/PuneCon55413.2022.10014893.

[10] Zellar, P. I. . (2021). Business Security Design Improvement Using Digitization. International Journal of New Practices in Management and Engineering, 10(01), 19–21. https://doi.org/10.17762/ijnpme.v10i01.98

[11] Prof. Rathod V U Raisoni: N. P. Sable, V. U. Rathod, P. N. Mahalle and D. R. Birari, "A Multiple Stage Deep Learning Model for NID in MANETs," 2022 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2022, pp. 1-6, doi: 10.1109/ESCI53509.2022.9758191.

[12] Prof. Rathod V U Raisoni: N. P. Sable, M. D. Salunke, V. U. Rathod and P. Dhotre, "Network for Cross-Disease Attention to the Severity of Diabetic Macular Edema and Joint Retinopathy," 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2022, pp. 1-7, doi: 10.1109/SMARTGENCON56628.2022.10083936.

[13] Prof. Rathod V U Raisoni: Vijay U. Rathod* & Shyamrao V. Gumaste, "EFFECT OF DEEP CHANNEL TO IMPROVE PERFORMANCE ON MOBILE AD-HOC NETWORKS", J. Optoelectron. Laser, vol. 41, no. 7, pp. 754–756, Jul. 2022.

[14] Christopher Davies, Matthew Martinez, Catalina Fernández, Ana Flores, Anders Pedersen. Applying Recommender Systems in Educational Platforms. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/171

[15] Prof. Rathod V U Raisoni: V. U. Rathod and S. V. Gumaste, "Role of Neural Network in Mobile Ad Hoc Networks for Mobility Prediction", Int. j. commun. netw. inf. secur., vol. 14, no. 1s, pp. 153–166, Dec. 2022.

[16] Mangesh D. Salunke, Ruhi Kabra, "Denial-of-Service Attack Detection", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 11.

[17] Mangesh D. Salunke, Ruhi Kabra, Ashish Kumar, "Layered architecture for DoS attack detection system by combine approach of Naive bays and Improved K-means Clustering Algorithm", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 03 | June-2015.

[18] Salunke M.D, Kumbharkar P.B., YK Sharma, "A Proposed Methodology to Prevent a Ransomware Attack", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-1, May 2020.

[19] Wiling, B. (2021). Locust Genetic Image Processing Classification Model-Based Brain Tumor Classification in MRI Images for Early Diagnosis. Machine Learning Applications in Engineering Education and Management, 1(1), 19–23. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/6

[20] Salunke M.D, Kumbharkar P.B., YK Sharma, "A Survey on Ransomware attack: Detection Technique", Dogo Rangsang Research Journal www.drsrjournal.com ISSN: 2347-7180 Vol-10 Issue-06 No. 14 June 2020.

[21] Prof. Nilesh N. Thorat," Visual Cryptography Schemes for Secret Colour Image Sharing using General Access Structure and Stamping Algorithm", International Journal of Engineering Research & Technology (IJERT", ISSN: 2278-0181, Vol. 4 Issue 03, March-2015.

[22] Maria Gonzalez, Machine Learning for Anomaly Detection in Network Security , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[23] Prof. N. N. Thorat," Embedded Visual Cryptography for Secret Colour Images Sharing using Stamping Algorithm, Encryption and Decryption technique", IJARCCE, ISSN (Online) 2278-1021, Vol. 5, Issue 2, February 2016.

[24] Prof. Rathod V U Raisoni: V. U. Rathod and S. V. Gumaste, "Role of Deep Learning in Mobile Ad-hoc Networks", IJRITCC, vol. 10, no. 2s, pp. 237–246, Dec. 2022.

[25] Prof. Rathod V U Raisoni: N. P. Sable, V. U. Rathod, P. N. Mahalle, and P. N. Railkar, "An Efficient and Reliable Data Transmission Service using Network Coding Algorithms in Peer-to-Peer Network", IJRITCC, vol. 10, no. 1s, pp. 144–154, Dec. 2022.