ISSN 2395-1621

# Embedded Visual Cryptography for Secret Color Images Sharing through Stamping Algorithm and OTP process

[#1]Prof. N.N.Thorat, [#2]Raju U. Jondhale, [#3]Lokesh B. Dandgole,
[#4]Ravi R. Wadikar

[1]nileshthorat4694@gmail.com
[2]rajujondhale35@gmail.com
[3]lokeshdandgole1993@gmail.com
[4]raviwadikar23@gmail.com

[#1234]Department of Information Technology,

JSPM"s Bhivarabai Sawant Institute of Technology &Research,
Pune University, India.

**ABSTRACT**

**Today's world with the growth of digital media, it is becoming more prevalent to find a method to protect the security of that media. An effective method for securely transmitting images is found in the field of Visual Cryptography (VC). Visual cryptography uses the characteristics of human vision to decrypt encrypted images. Sharing of secret information via emails is not that much secure as the information or data can be hacked easily by the third-party. In this current work we have proposed Visual Cryptographic Scheme for color images where the divided shares are enveloped in other images using stamping. The shares are generated using Random Number. Visual Cryptography Schemes (VCS) is a process of encrypting the image which hide the secret information present in images. In simple visual cryptographic technique encryption of secret image is done by splitting the image into n number of shares and the Stamping process is performed by overlapping k number of shares. It may helps to hide secret image. The decryption process of simple visual cryptographic system can be performed by a human eye so there is a possibility of security issues while using cryptography for sharing information and to solve this problem we are using OTP process. Earlier static ID and Password are used which is vulnerable against eavesdropping and replay attack. To overcome this problem One Time Password technique is used which give different password each time. Previous methods faced some security issues like pixel expansion and noise troubleshoot the proposed system add more security to generated transparencies by applying an envelope to each shares by using stamping algorithm**

**Keywords: Visual Cryptography, stamping algorithm, OTP (One-Time-Password), shares**

ARTICLE INFO

**Article History**

Received: 16th March 2017

Received in revised form :

16th March 2017

Accepted: 18th March 2017

**Published online :**

**19th March 2017**

## I. INTRODUCTION

It is now common to transfer multimedia data via the Internet. With the coming era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment. With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography was introduced by Naor and Shamir in the year 1994. Visual Cryptography is a type of encryption technique to conceal the information in images and decryption can be performed by the human eye if the proper key images are used. Visual cryptography is the concept of dividing a secret image into "n" shares and revealing secret image by stacking a qualified subset of "n" shares. It is difficult to fetch the information from one of the share. Acceptable number of

 

transparent shares is needed to disclose the information. The simplest way to implement this scheme is to stamp the two layers onto a transparent sheet. . In Visual Cryptography Scheme (VCS) picture or text should be given as an input in the form of digital images to the system and the system forms „ n‟ (2<n) number of several images (called shares), which looks like images of random noise. The user has to load „ k‟ number of shares, where 2<k<n, from those „ n‟ number of shares to reveal the secret image. The main feature of this approach is that the secret image is decrypted easily by the human visual system without performing any complex calculation. Naor and Shamir‟s scheme can conceal the secret image in n distinct images called shares. The secret image can then be revealed by easily loading together as many as k of the shares. Each of the shares looks like a set of random pixels. Generally, any single share, before being loaded up with the others, discloses nothing about the secret image. By using the stamping algorithm in Ref the shares are meaningful if the secret is binary. But in the case of color secret image the shares a partially meaningful due to high amount of random pixels. So in the proposed system a digital watermarking technique is used for stamping a cover image to the random share without any pixel expansion. The cover images are color images that are represented by 24 bits (8 bits in each plane). The random looking shares are represented by 8 bits. The proposed scheme digitally watermarks these 8 bits of a pixel into the 24 bit pixel of the cover image. This can be done by replacing the b Least Significant Bits (LSB) of each plane of the cover image. The decryption process of simple visual cryptographic system can be performed by a human eye so there is a possibility of security issues while using cryptography for sharing information and to solve this problem we are using OTP process.

One time password generator is an algorithm that generate new random password every time. It works as a machine or algorithm that takes input from users and produce new password that is different from previously generated password. Network security deals with authenticate the user with id and password but this method is vulnerable to many attacks so for secure authentication every time new password is used whether the previous password is stolen or misplace. One time password generator is main element of One Time Password system used for generating the generating random passwords other elements of this system is client authentication and Server authentication. Popular OTP used are HOTP based on SHA-1. Hash algorithms used are MD4, MD5 but these are vulnerable to attacks. Another OTP is based on Ping Pong-128 stream cipher in which Ping Pong-128 algorithm is used to generate the random numbers.

One time password is secured because:
1. It can't used twice or
2. It is not reversible to reach at source back.

It mainly deals with the two elements
1. Key
2. Counter

OTP system generates one password at a time and provides it to client for authentication. OTP send password to client by SMS service, by phone or by written. Password is secure by the application on client mobile.

## II. EXISTING SYSTEM

Haibo Zhang, Xiaofei Wang, "Visual Cryptography for General Access Structure by Multi-pixel Encoding with Variable Block Size.", 2004.

Multi-pixel encoding is a developing technique in visual cryptography which encodes more than single pixel for each run. In fact on the other hand its ability of encoding is poor. This paper put forth a novel multi-pixel encoding which could encode several numbers of pixels for each run. The size of encoding at single run is parallel to the number of the continuous same pixels discovered during scanning of secret image. The proposed technique can work efficiently for chromatic images and general access structure without pixel expansion. The experimental results also show that it could accomplish high efficiency for encoding and better quality for overlapped images.

Z. Zhou, G. R. Arce, and G. Di Crescenzo.,"Halftone Visual Cryptography." 2007.

Visual cryptography conceals a secret binary image (SI) into shares of random binary order. If the shares are stamped onto transparencies, the secret image could be visually decrypted by overlapping a definite subset of transparencies. However, no secret information could be achieved from the overlapping of a closed subset. The binary structure of the shares, however, has no visual meaning and bottlenecks the objectives of visual cryptography. Extended visual cryptography was suggested recently to build up meaningful binary images as shares using hyper graph colorings, but the visual quality was very low. In this paper, a technique known as halftone visual cryptography is introduced to obtain visual cryptography via half toning.

The simulation shows that the visual qualities of the generated halftone shares are better than any other available visual cryptography technique known to date.

Ming Sun Fu. Oscar C. Au., "Joint Visual Cryptography and Watermarking", 2005.

The hidden image can only be disclosed when sufficient share images are achieved. For watermarking, the hidden image is embedded in one halftone image while maintaining the quality of the watermarked halftone image. In this paper, Ming Sun Fu proposed a joint Visual-cryptography and watermarking (JVW) algorithm that has the advantages of both watermarking and visual cryptography.

D.Parameswari , L.Jose, "SET with SMS OTP using Two Factor Authentication", 2007.

This paper describes a method of implementing two factor authentication using SMS OTP - One Time Password to Secure an Transaction (SET). The proposed method guarantees authenticated transactions in services, such as online banking, e-shopping or ATM machines. The proposed system involves generating and delivering a One Time Password (OTP) to a mobile phone in the form of SMS - Simple Messaging Service. The generated One Time Password is valid for only a short user defined period of time and it is generated and verified using Secured Cryptographic Algorithm. The proposed method has been implemented and tested successfully.

 

## III. PROPOSED METHODOLOGY

**Visual Cryptography**

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human visual system. The benefit of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into a number of parts let n. k-n secret sharing scheme is a special type of Visual Cryptographic technique where at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information while decryption the receiver will need a password to decrypt image.

**Stamping Cover Images**

The most VCS produce the random noise like shares as output. The hackers are more interested in this type of random shares and these shares are difficult to recognize by the participants. To recover from these difficulties the proposed scheme uses meaningful shares. By using the stamping algorithm in Ref the shares are meaningful if the secret is binary. But in the case of color secret image the shares a partially meaningful due to high amount of random pixels. So in the proposed system a digital watermarking technique is used for stamping a cover image to the random share without any pixel expansion. The cover images are color images that are represented by 24 bits (8 bits in each plane). The random looking shares are represented by 8 bits. The proposed scheme digitally watermarks these 8 bits of a pixel into the 24 bit pixel of the cover image. This can be done by replacing the b Least Significant Bits (LSB) of each plane of the cover image. The proposed digital watermarking technique used for stamping is listed in Algorithm 2.

**One Time Password**

One time password generator is an algorithm that generate new random password every time. It works as a machine or algorithm that takes input from users and produce new password that is different from previously generated password. Network security deals with authenticate the user with id and password but this method is vulnerable to many attacks so for secure authentication every time new password is used whether the previous password is stolen or misplace. One time password generator is main element of One Time Password system used for generating the generating random passwords other elements of this system is client authentication and Server authentication. OTP system generates one password at a time and provides it to client for authentication. OTP send password to client by SMS service, by phone or by written. Password is secure by the application on client mobile.

**Overall Process**

**Step I:** The source image is divided into n number of shares using k-n secret sharing visual cryptography scheme such that k number of shares is sufficient to reconstruct the encrypted image.

**Step II:** Each of the n shares generated in Step I is embedded into n number of different envelope images using LSB replacement.

**Step III:** k number of enveloped images generated in Step II are taken and by using a OTP and LSB retrieving with OR operation, the original image is reconstruct.

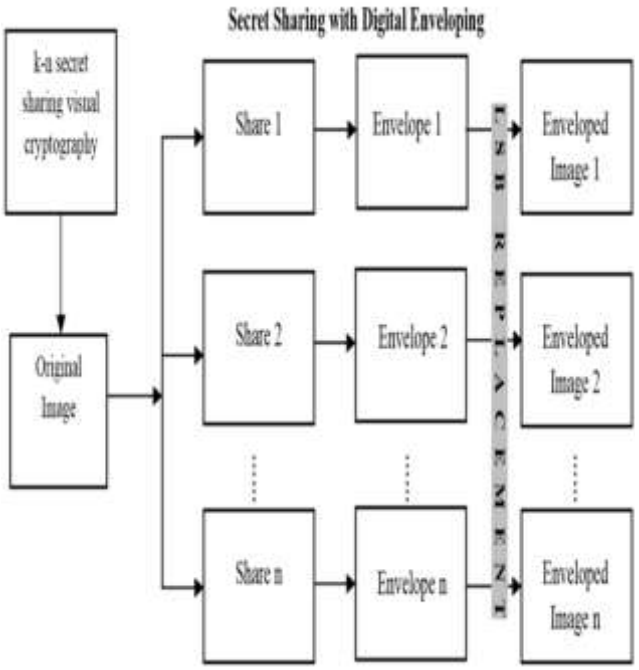


**Fig 1. System Architecture**

1. **Encryption Process**

It consists of generation of shares using any basic visual cryptography model. In our proposed scheme, a (2, 2) VC share creation is performed. Each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub pixels. A black pixel is shared into two complementary blocks of four sub pixels. All the pixels in the secret image are encrypted similarly using this scheme. The shares can be either Vertical, Horizontal or Diagonal shares. Any single share is a random choice of two black and two white sub pixels, which looks medium grey. When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black). The visual secret sharing scheme assumes that the message consists of a collection of colour pixels and each pixel is handled separately. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m sub pixels, which are printed in close proximity to each other so that the human visual system averages their individual contributions.

2. **Decryption Process**

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.In this step all n numbers of enveloped images

 

are considered as input. Where each of these images for each pixel, the last two bits of alpha, red, green and blue (RGB) are retrieved and OR operation is performed to get the original image. The logic is that human visual system is acts as an OR function. For generated process the OR function can be used for the case of stacking n number of enveloped images.

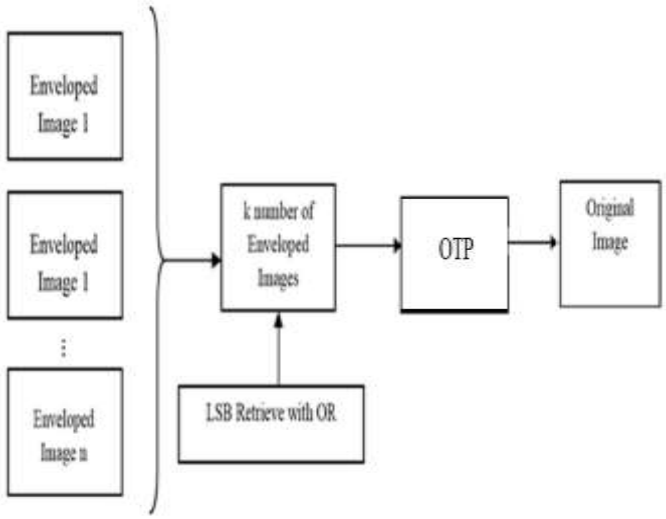


Fig 2. Process flow

**3. OTP Process**

One time password generator is an algorithm that generate new random password every time. It works as a machine or algorithm that takes input from users and produce new password that is different from previously generated password. Network security deals with authenticate the user with id and password but this method is vulnerable to many attacks so for secure authentication every time new password is used whether the previous password is stolen or misplace. One time password generator is main element of One Time Password system used for generating the generating random passwords other elements of this system is client authentication and Server authentication. Popular OTP used are HOTP based on SHA-1.Hash algorithms used are MD4, MD5 but these are vulnerable to attacks. Another OTP is based on Ping Pong-128 stream cipher in which Ping Pong-128 algorithm is used to generate the random numbers.

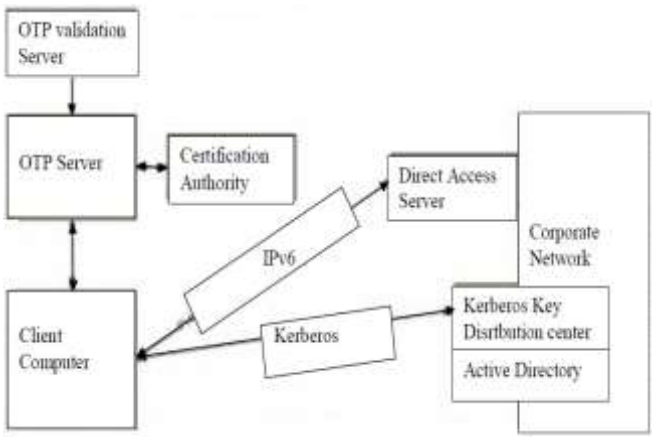


Fig 3. OPT generation

## IV. ALGORITHM

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

An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The division is done by the following algorithm.

**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)
```

 

{
Generate a random number within n, let rand_int. [9]
if (rand_int is not in RAND [RECONS]) RAND [i] = rand_int
}
return RAND [RECONS]
}

**2. Encryption Algorithm: -**
An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The encryption, i.e. division of the image into n number of shares such that k numbers of shares are sufficient to reconstruct the image; is done by the following algorithm.

**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.

**3. k-n Secret Sharing Of the Original Image Using Random Sequence 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)**Initialize 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 ns.
Perform OR between the ith bit of Sj share
(where 1 j n) with the jth bit of the sequence Sqr ,
(1 r ns).
}

**4. Proposed Stamping Algorithm:**
Procedure Stamping (Shares, Covers)
1. Repeat for all shares
2. Repeat for each pixel of share

i) Generate an array S[0…8] that contain the bits of a pixel value
ii) Decompose the color 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.

iii) Find that which channel contain more information, i.e which color has less effect in the cover image.

iv) 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.
3. Stop

**5. Decryption Algorithm: -**
In this step at least k numbers of enveloped images are taken as input. From each of these images for each pixel,the last two bits of alpha, red, green and blue are retrieved and OR operation is performed to generate the original image. It is already discussed that human visual system acts as an OR function. For computer generated process; OR function can be used for the case of stacking k number of enveloped images out of n. The ecryption process is performed by the following algorithm.

**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 bitwise 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 substring from FINAL[ ] starting from 0.

Construct pixel from these part and store it into IMG_CONS[(w/4)*h]

Generate image from IMG_CONS[ ].

**6. OTP Algorithm: -**

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it is very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micro payments In this *n* participants hold shares generated from secret *S*. A (k, n) threshold scheme is followed, where any information about *S* cannot be obtained from *k-1* or less shares. *S* can be recovered only from *K* and more shares.

A fast (2, n) threshold is used here, where we could get *S* just by XOR operation. This was
proven fast and secure.

In this scheme we generate a random number and divide secret into 4 shares by making XOR. Then we encrypt and deliver one share to user in the form of SMS.

If he is a valid user, then he will provide approval by typing the OTP during transaction approval. Then that share is decrypted and compared with the other share which is stored in the database. Thus this Threshold Secret Sharing Scheme (TSSS) helps to generate a Secured and Random OTP.

**1.** When user login servers take its Email ID and Password and authenticate the user.

**2.** Server simply encrypts the Id and password and gives that output to OTP generator.

**3.** OTP generator starts its work. OTP selects two alphabets from encrypted data and use genetic algorithm.

**4.** By using genetic operators we create random 8 alphabets from that two alphabets and suppose it is Random key.

**5.** We have to select 8 alphabets from encrypted output assume it as ID.

**6.** Now we have two keys of 8 alphabets. One is Random key and second is
Identification ID.

**7.** Divide Identification ID and Random password into two halves of 4 alphabets. i.e. pswdL = X1X2X3X4 pswdR = X5X6X7X8 IDL = Y1Y2Y3Y4 IDR = Y5Y6Y7Y8

**8.** Take random point from elliptic curve which satisfy equation of elliptic curve and convert it into binary form of 8 bits.

**9.** Now according to the binary value perform steps. If b[i] ==0 perform KL = pswdL (OR operation) IDL KR = pswdR (OR operation)IDR Else if b[i] ==1 perform KL = pswdL (OR operation) IDL KR = pswdR (OR operation) F(IDR)
Where F (IDR) = Product between the IDR and Any random point in elliptic curve.

**10.** Merge KL AND KR is equal to K.

**11.** Merge F (IDR) and IDL = ID.

**12.** Find the product of ID with any private key.

**13.** We have now 8 Random passwords which we are store in database and newly generated identification No. (ID).

**14.** Next time when user login then that Identification No. (ID) is given to OTP generator for generating password.

## V. CONCLUSION

In this current work, with well-known k-n secret sharing visual cryptography technique an enveloping method is introduced where the secret shares are enveloped within clearly innocent covers of digital images using LSB replacement. This gives protection to visual cryptography scheme from unlawful attack as it fools the hacker's eye. Decryption process of simple visual cryptography is based on human vision system, so if a person gets competent k number of shares; the image can be easily decrypted using OTP. One time password is an efficient technique that generate random password each time for users. If user lost their pervious password then there is no need of worry for them because OTP give them new password for each session. OTP prevent user id from replay or eavesdropping attack. The splitting of an image into n number of shares is done by using random number generator.

## REFERENCES

**[1]** M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology- Eurocrypt‟94,1995.

**[2]** P. Ranjan, "Principles of Multimedia", Tata McGraw Hill, 2006.

**[3]** John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.

**[4]** Kandar Shyamalendu, Maiti Arnab, "K-N Secret Sharing Visual Cryptography Scheme For Color Image Using Random Number" International Journal of Engineering Science and Technology, Vol 3, No. 3, 2011, pp. 1851-1857.

**[5]** Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University, 2010, pp 62-65.

**[6]** Nakajima M, Yamaguchi Y, Extended Visual Cryptography for Natural Images, 10-th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision'2002.

 