ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Embedded Visual Cryptography for Secret Color Images Sharing Through Stamping Algorithm and OTP Process

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

Professor, Department of Information Technology, JSPM‟s Bhivarabai Sawant Institute of Technology &Research, Pune University, India.[1]

B. E Students, Department of Information Technology, JSPM‟s Bhivarabai Sawant Institute of Technology &Research, Pune University, India.[2]

ABSTRACT: Today's world with the growth of digital media, it is becoming more prevalent to finda method to protect the security of that media. An effective method for securelytransmitting images is found in the field of Visual Cryptography (VC). Visualcryptography uses the characteristics of human vision to decrypt encrypted images.Sharing of secret information via emails is not that much secure as the information ordata can be hacked easily by the third-party. In this current work we have proposedVisual Cryptographic Scheme for color images where the divided shares areenveloped in other images using stamping. The shares are generated using RandomNumber. Visual Cryptography Schemes (VCS) is a process of encrypting the imagewhich hide the secret information present in images. In simple visual cryptographictechnique encryption of secret image is done by splitting the image into n number ofshares and the Stamping process is performed by overlapping k number of shares. Itmay helps to hide secret image. The decryption process of simple visual cryptographicsystem can be performed by a human eye so there is a possibility of security issueswhile using cryptography for sharing information and to solve this problem we areusing OTP process. Earlier static ID and Password are used which is vulnerableagainst eavesdropping and replay attack. To overcome this problem One TimePassword technique is used which give different password each time. Previousmethods faced some security issues like pixel expansion and noise troubleshoot theproposed system add more security to generated transparencies by applying anenvelope to each shares by using stamping algorithm.

KEYWORDS: Visual Cryptography, stamping algorithm, OTP (One-Time-Password),shares.

I. INTRODUCTION

1.1 Visual Cryptography

Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers .Image is a multimedia component sensed by human perception. Pixel is the smallest unit constructing a digital image. Each pixel of a 32 bit digital color image are divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. If all bits of Alpha part are „0‟, then the image is fully transparent.A 32 bit sample pixel is represented in the following figure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

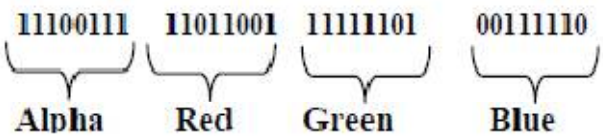


Fig 1: Structure of a 32 bit pixel

Structure of a 32 bit pixel Human visual system acts as an OR function. If two transparent objects are stacked together, the final stack of objects will be transparent. Changing any of them to non-transparent, the final stack of objects will be non-transparent.

1.2 SENTIMET ANALYSIS

To add more security to the secret sharing of the image Invisible Digital Watermarking is used which protects the secret image from the hacker. For the decryption process a key is used which includes the Number of share required to decrypt the secret image and the envelop images which are used in the encryption process.The division of an image into n number of shares is done by using random number generator, which is a new technique not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images. This technique only checks '1' at the bit position and divide that '1' into (n-k+1) shares using random numbers. A comparison is made with the proposed scheme with some other schemes to prove the novelty of the scheme.

II. RELATED WORK

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts. In the table on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

1. Encryption

The secret image is first divided into channel images and color error diffusion technique is applied for dithering to improve the quality of image. This technique produces better results as compared to other dithering techniques. In this describes the overall encryption process. Section III describes the key generation and the secure sending of the key to the destination. Section IV defines the overall decryption phase

2. Decryption

The decryption process is the reverse process of the encryption process. In the decryption process the shares are stacked together and the block is sub sampled in such a way that it is converted into a single pixel and the size of the decrypted image is same as the original image. Firstly, it involves the retrieval of the key at the receiving side and getting all the information about the number of shares and envelops images. Once the key is retrieved, we identify the enveloped images and remove the watermark from the shares In this chapter we will see various studies and researches conducted in order to identify current scenarios andtrends in hiding the images using visual cryptography. In literature Survey we are going to study Existingsystems which are use in Visual cryptography system. These Systems are:

2.1 Shamir's Secret Sharing Scheme

The Shamir's secret scheme divides a secret data S into n number of shares let be S1, S2. . . . .,Sn. such that

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

1. Values of k or more shares among Si (i n) can retrieve the secret information.
2. Values of less than k shares retrieve no information about the secret share.

This type of technique is called (k, n) secret sharing algorithm. This technique is described with an example inthe following parts. The (k, n) secret sharing comes from the concept that k number of points are necessary todefine a polynomial of degree (k=1). To construct the polynomial, (k=1) coefficients a1, a2,. . . .,ak=1 areneeded.Here a0= S, the secret data. The polynomial f(x) = a0 + a1x +a2x2 +, …,+ak=1xk=1 is constructed from the coefficients. Total n points i.e. let I = 0. . . ..Nare taken andcorresponding f(x) are also be calculated. From values n number of pairs (i, f (i)) is constructed. The originalcoefficients can be retrieved by interpolation method from at least k numbers of these pairs.

2.2 Blakley Secret sharing scheme

Blakley secret sharing is based on hyper plane. It is a true that non-parallel lines intersect at a specific point.
This secret sharing scheme says that,
1. Secret is point is must in m-dimensional space.
2. Share corresponds to only a hyper plane.
3. Intersection of threshold planes gives the secret values.
4. Less than threshold planes will not intersect to the secret values.

2.3 Asmuth-Bloom secret sharing scheme

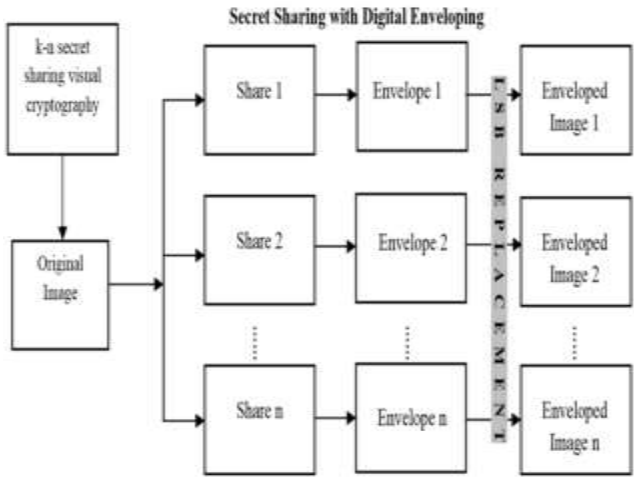
This technique is based on Chinese Remainder theorem. This technique takes a sequence of pair in co prime integers p0, p1, . . .,pn such that where n > 2 and 2 k n. The working principle of this scheme is as following:
1. The secret S is chosen as a random element from the set Z.
2. A random integer a is chosen such that S + ap0 < p1p2,…,pk.

The reduction modulo mi of S + ap0 for all 1 i n is calculated. These are represents shares i.e. following. Ii =(Si, pi).
3. From given k distinct shares Ii1 , . . . , Iike, the following set of equations are formed As pi1, pi2, ...pik.

The secret S is the reduction module p0 of S0.

Recently in the literature, many new methods have been implemented for visual cryptography. In 1994 Naor and Shamir, have developed the Visual Secret Sharing Scheme (VSSS) to implement this model. In theprevious system called n-n sharing visual cryptography scheme, the image can be retrieved even if only k sharesare available, this is a major security issue. In our proposed system, the image can be retrieved only if all nshares of images are available. Apart from this, we use random number generator for generating shares ofimages. From above Literature survey, we found some limitations & drawbacks of visual cryptography usingcomplex number system that it does not provide more security to organization & it Uses complex numberalgorithm for black and white images. Proposed System will provide the random number for encryption anddecryption. It also uses digital watermarking for security purpose

III. ARCHITECTURE



(a)

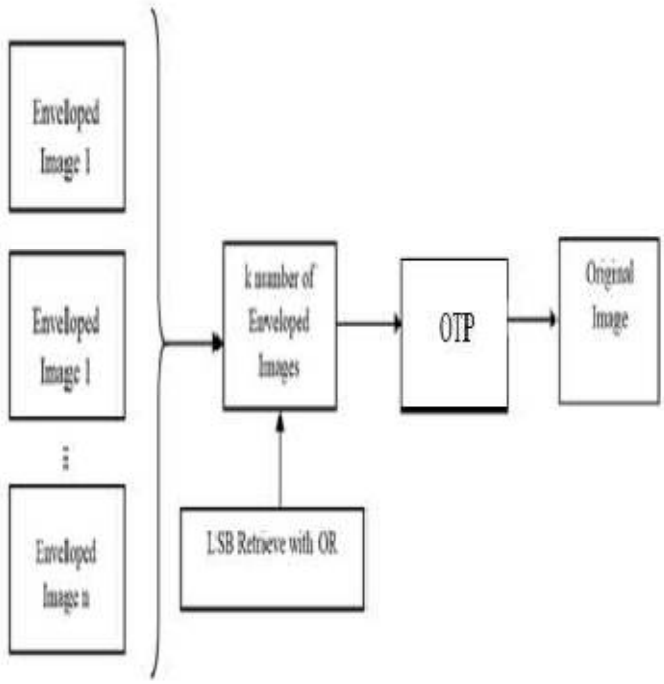
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017



(b)

Fig. 02 (a,b)System Architecture

IV. IMPLEMENTATION

1. PRE-PROCESSING OF VISUAL CRYPTOGRAPHY

In this section, we examine the application of the preprocessing schemes to construct a dividing scheme without image size expansion. In doing so, we take images as inputs. The first image is considered to be meaningful cover images and the third image is the secret image. One of the block replacement algorithms converts the three input images into the processed images. A processed image contains white and black blocks and can be used as an input secret image in any visual cryptography encoding process. After producing the three processed images by the appropriate method, the two shares are generated according to the encoding process specified in. The secret image is recovered by stacking the two shares together. It should be noted that our non-expansion EVC scheme is as secure as the scheme introduced in, as the new scheme does not change the share generation approach..

2. MODULES

1) Encryption Module

In this Module Using this step the divide number of shares of the original image are enveloped within other different image. Least Significant Bit (LSB) replacement using digital watermarking is used for this enveloping process. It is already discussed that a 32 bit digital image pixel is divided into four parts that are following,

1. Alpha
2. Red
3. Green
4. Blue

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Each bit made of 8 bits. Experiment shows that if the last two bits of each of these parts are changed, then the changed color effect is not visible by human eye. This overall process is known as digital watermarking.

2) Decryption Module

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.

a. **TWEET SENTIMENT SCORING**
b. **STRESS PREDICTION DATA PRE-PROCESSING**

A) Visual Cryptography Analysis

Data security has become a most important issue in data communication especially in the field of Computer Network. The data can have many forms such as text, image, and sound etc. There are many cryptosystems exists to protect data out of those Visual Cryptography (VC) is a popular technique to protect image based data. It splits the secret image into shares in encryption process and the original image can be retrieved by stacking the required number of shares at the time of decryption. Steganography is another method of cryptosystem used to protect data. It hides the secret inside another data. It makes the secret invisible to users. But in the rapid expansion of cryptanalysis, data is still very insecure in some state of affairs. Hence, to provide a strong security mechanism a hybrid approach using the feature of VC and encryption and decryption techniques is wise to adopt. This paper studies the visual cryptography scheme, new secrete sharing scheme and various hybrid approaches for data security especially for image based data

B) Algorithm: Stamping Algorithm

INPUT: Shares and covering images
OUTPUT: Embedded image
METHOD: Procedure Stamping (shares, cover images)
STEP 1: Calculate the collection of pixel colors for shares, cover images and secret image in coordinate (x, y)
STEP 2: Calculate required amount of cover pixels in shares in black and white region of the secret image
STEP 3: Calculate the amount of black pixels overlapped at coordinate (x, y)
STEP 4: Set the indicator for coordinate to 0 i.e.., available for stamping cover pixel.
STEP 5: Add cover pixels on selected coordinates (x, y) of shares. The black pixels will be added on candidate coordinate (x, y) of share that has a white pixel on it.
STEP 6: Repeat from step 3 to step 5 until all require cover pixels are stamped on shares

V. RESULT AND EVALUATION

1)Upload Image

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

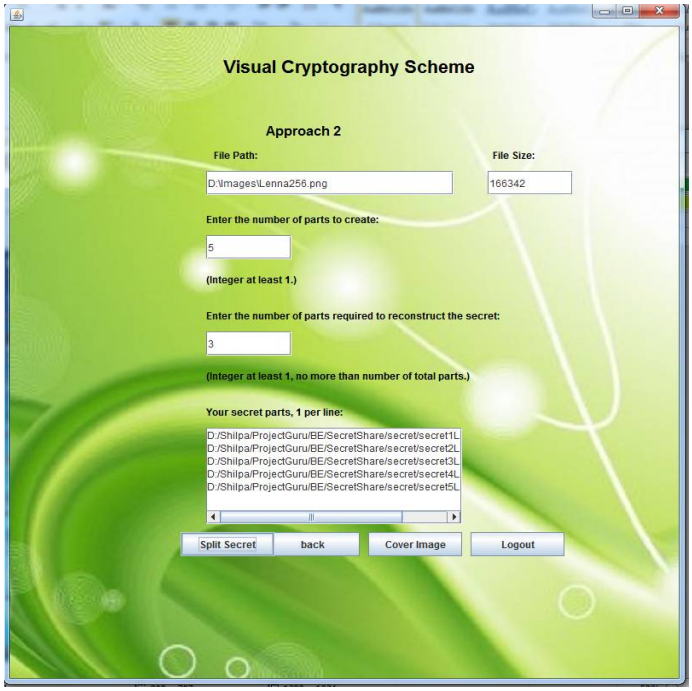
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

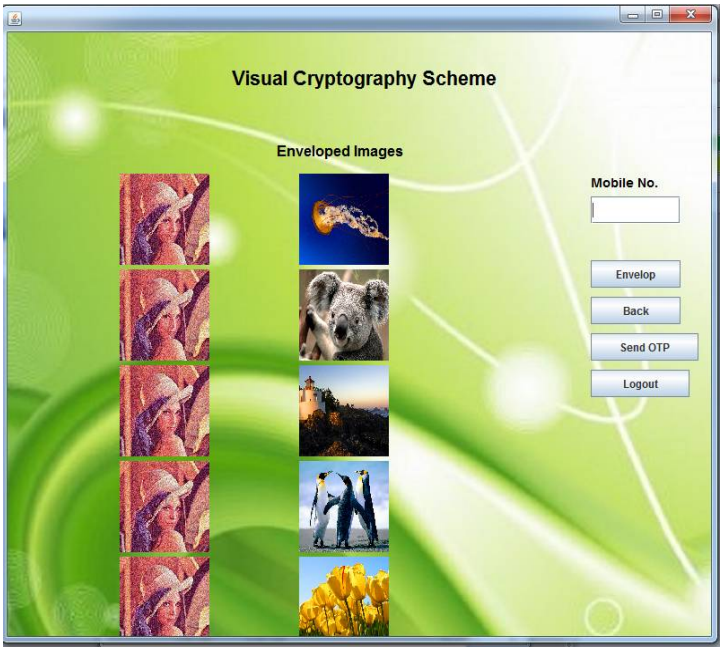
Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

2)Secret Generation



3) Secret Images and Cover Images



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

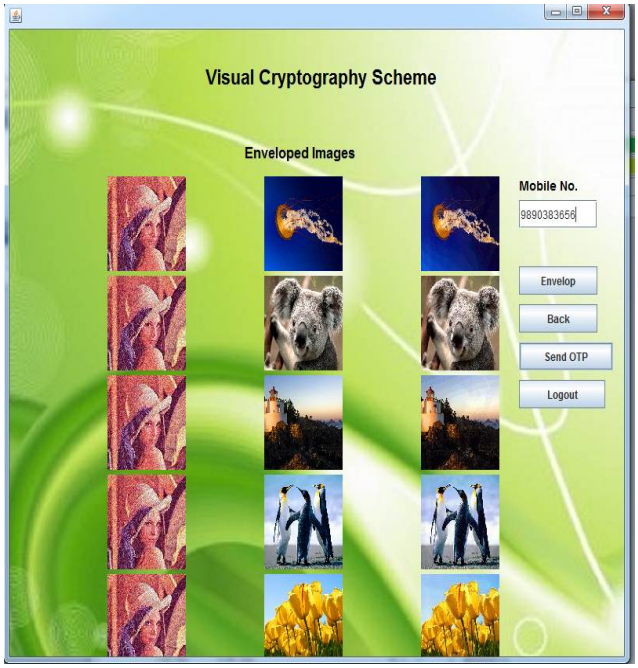
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

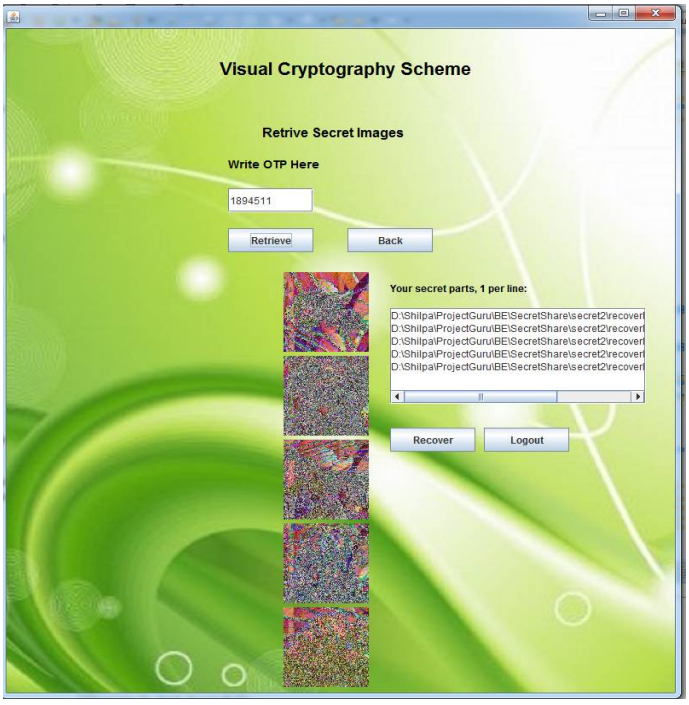
Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

4)Enveloped Images



5)Recovered Secret Images



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

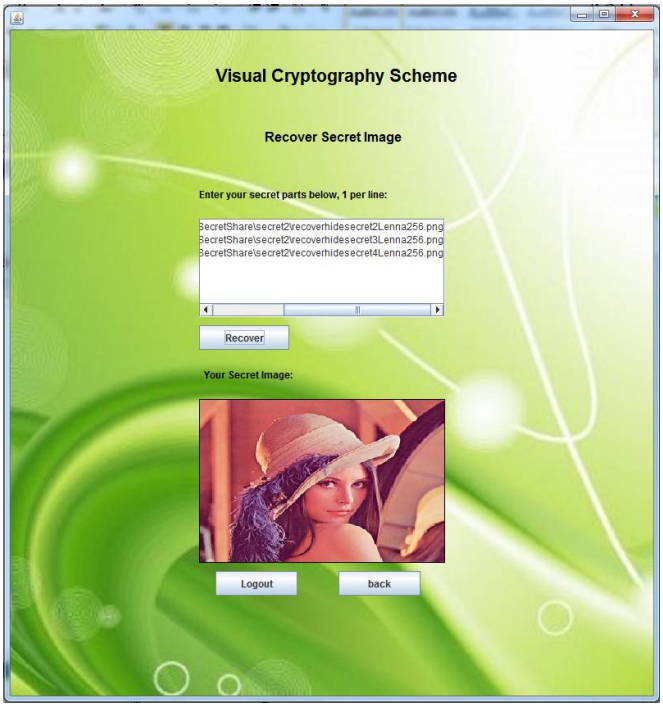
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

6)Recover Origin image



In this section, we examine the application of the preprocessing schemes to construct a dividing scheme without image size expansion. In doing so, we take images as inputs. The first image is considered to be meaningful cover images and the third image is the secret image. One of the block replacement algorithms converts the three input images into the processed images. A processed image contains white and black blocks and can be used as an input secret image in any visual cryptography encoding process. After producing the three processed images by the appropriate method, the two shares are generated according to the encoding process specified in. The secret image is recovered by stacking the two shares together. It should be noted that our non-expansion EVC scheme is as secure as the scheme introduced in, as the new scheme does not change the share generation approach. In that we use K N secrete sharing scheme for visual encryption and decryption in visual cryptography.

VI. CONCLUSIONANDFUTURE WORK

Decryption part of visual cryptography algorithm is based on OR operation, so person gets sufficient k number of shares. The image can be easily decrypted using k-n secret sharing algorithm. In this work, with well-known k-n secret sharing using visual cryptography scheme an enveloping technique is used where the secret shares are enveloped within images using Least Significant Bit replacement digital watermarking this providing security to visual cryptography technique from malicious attack.

In Future Work Visual Cryptography technique is used to protect image-based secret information. In this scheme we have proposed a technique called random sequence to divide an image into n number of shares. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimizes. But the distorted shares may arise suspicion to the hacker's mind that some secret information is passed. The original image can be encrypted using a key to provide more security to this scheme. The key may be a text or a small image. Steganography can be used by enveloping the secret shares within apparently innocent covers of digital picture. This technique is more effective in providing security from illicit attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

REFERENCES

[1] International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013 1 ISSN2250-3153.
[2] International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 1 Jan 2013 Page No. 265-303.
[3] IJCSNS International Journal of Computer Science and Net- work Security, VOL.12 No.12, December2012.
[4] International Journal of Computer Applications (0975 § 8887) Volume 25§ No.11, July 2011.
[5] IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.
[6] KandarShyamalendu, MaitiArnab, 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.
[7] International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.
[8] Kang InKoo el. at., Color Extended Visual Cryptography using Error Diusion, IEEE 2010.
[9] Journal of Computing, Volume 2, Issue 4, April 2010, ISSN 2151-9617.
[10] SaiChandana B., Anuradha S., A New Visual Cryptography Scheme for Color Images, International Journal of Engineering Science and Technology, Vol 2 (6), 2010.
[11] M. Naor and A. Shamir, "Visual cryptography", Advances in Cryptology-Eurocrypt'94, 1995, pp.1-12
[12] Schildt, H. The Complete Reference Java 2, Fifth Ed. TMH, Pp 799-839.
[13] Krishmoorthy R, Prabhu S, Internet & Java Programming, New Age International, pp 23.
[14] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.