Authenticated color extended visual cryptography

Authenticated Color Extended Visual Cryptography with Perfect Reconstruction

R. Sathishkumar, Gnanou Florence Sudha

A

Abstract – Visual Cryptography Scheme (VCS) is an image safeguarding scheme which encrypts the secret text based image into multiple binary images called shares, which are then transmitted to participants. These shares are then stacked over by the participants to decrypt the secret image, however with reduced quality. In Extended Visual Cryptography Scheme (EVCS), these binary shares are encoded with cover images to generate meaningful shares. In order to enhance the decoded EVCS secret image quality, Two in One Image Secret Sharing Scheme (TiOISSS) was implemented, which offers perfect retrieval of the secret image. In this proposed scheme, the TiOISSS implemented for color secret image with meaningful color shares with perfect reconstruction is proposed. This scheme uses Adaptive Halftoning technique to improve the EVCS image quality. Further, a color authenticated image and a text message are encoded in the meaningful color shares to suppress any fake shares from the intruders, thus improving the security of the proposed scheme. Experimental results depict that the improvement in quality and security of the scheme.

Index Terms – Image Security, Visual Cryptography Scheme, Adaptive Halftone, Polynomial Image Secret Sharing,

I. A, A Introduction

With the swift development in the networking technologies, digital data are transmitted across the world over internet. Thus, security has become a vital issue in both communication and the complex encryption gives ways to secure the information from the intruders. Image encryption has a vital role in variety of applications like telemedicine, medical image processing, military applications, etc. In the traditional way of encryption, the data will be encrypted with a security key and the decryption must be done with the same key. Hence, the security key is essential for proper decoding of the secret data.

VCS is one such encryption method proposed by Naor and Shamir [1-2] to hide a secret image in the form of *n* noisy pictures called shares such that the secret data is retrieved by Human Visual System (HVS) by stacking the *n* shares. The traditional VCS is relaxed for threshold VCS in which at least any *k* number of shares are sufficient to decode the secret image [3-4]. The VCS has been proposed to hide the gray images by suitably halftoning it to binary images [5-7]. These schemes were proposed with noisy shares, that may invite intruders’ attention.

R. Sathishkumar is with Department of Electronics & Communication Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology (PKIET), Karaikal, India. ()

Gnanou Florence Sudha is with Department of Electronics & Communication Engineering, Pondicherry Engineering College, Puducherry, India. ()

By suppressing this weakness, VCS were implemented with meaningful shares from the cover images, and is referred as Extended Visual Cryptography Scheme (EVCS) [8-9].

The VCS has further been extended for natural color images. Rijmen et al [10] proposed a VCS for color secret image with pixel expansion, in which each secret color pixel is expanded into a block of 2? 2 color sub-pixels to generate two color shares. Huo et al [11] proposed the VCS for gray-level and color images using color decomposition and halftone technology, while retaining the advantage of traditional monochrome visual cryptography. Huo et al [12-13] proposed an improved model by using binary encoding to represent the sub-pixel blocks. In [14], Huo et al adjusted the contrast to reveal the secret image with better quality, but the noisy shares reveal the secrecy of the image. Der et al [15] proposed a color VCS with an additional authentic image, but the scheme suffers from the visual quality.

Polynomial image secret sharing (PISS) was implemented with perfect decoding of secret image [16]. In [17], Sian et al implemented a Two in One Image Secret Sharing Scheme (TiOISSS) wherein the vague secret image is decoded using VCS in the 1st decoding stage and the better quality secret image is decoded using PISS using computations. Peng et al [18] improved the TiOISSS using GVCS with gray PISS values in the shares. Srividhya et al [19] improved the TiOISSS image quality by applying adaptive halftoning. However, the scheme is implemented for gray images with noisy shares. In [20], TiOISSS was implemented for meaningful shares, but the lossless recovery of the decoded image was not achieved. The existing model of

TiOISSS are implemented for gray images and generates noisy shares and that may invite the intruders to insert the fake shares.

In this proposed scheme, existing TiOISSS [20] is extended for natural color image with RGB color decomposition method. Further, before applying PISS algorithm, the color secret image is permuted at bit level, block level and pixel level to improve the security. This scheme generates meaningful shares based on the color cover images. A, A Additionally, a color authentication image and a textual secret message are shared to validate the authenticity of the decoded secret image.

Experimental results of the proposed scheme show that the weaknesses of the existing TiOISSS schemes are attempted, color TiOISSS are implemented with the enhanced quality and improved security.

This paper is organized as follows. The VCS for gray scale and color images, TiOISSS and its related works are discussed in section II. The proposed Authenticated Color VCS is discussed in section III. The experimental results are discussed in section IV. The Quality analysis and Security analysis are discussed in section V and section VI. The conclusion is presented in section VII.

II. A, A Related Works

The objective of the proposed scheme is to extend the TiOISSS for color images, with improved quality and perfect reconstruction. This section discusses the related works pertaining to existing TiOISSS and its limitations.

Visual Cryptography Scheme

Moni Noar and Adi Shamir implemented the visual secret sharing scheme in 1994 [1], which requires computations only in the encryption stage. The decoding of secret image is done by human visual system (HVS).

In *(k, n)* threshold visual secret sharing scheme, *n* noise like shares are generated. Any *k* or more number of shares are required to decode the secret image. With *(k-1)* or lesser shares, the secret cannot be reconstructed.

In basic (2, 2) VCS, every binary secret image pixel is expanded into 2? 2 sub-pixels in the 2 number of noisy shares, as per the sub-pixel coding table shown in Fig. 1. For every white pixelof the secret image, any one out of the six sub-pixels are randomly selected for both the shares. Similarly, for every black pixel of the secret image, any one out of the six sub-pixels are randomly selected for share 1, and its compliment sub-pixels for share 2.

Thus, by stacking the two shares, the white pixels are decoded with 50% gray level. However, the black pixels are reconstructed with full black sub-pixels. With the individual shares which has equal percentage of white and black pixels, the secret image information is not revealed. The share size and therefore the reconstructed image are doubled due to pixel expansion.

Fig. 1 Sub-pixel coding table

Adaptive Halftoning

Halftoning technique is a process of converting the continuous tone image to monochrome image or binary image. The VCS is generally suited for monochrome images. Many techniques like AM halftoning, FM halftoning,

etc. are available for converting the gray scale image to binary image. In [16-18], Error diffusion based on FM halftoning with is implemented. But, this results in scattered white pixels in the place of darker areas of gray image. The proposed work utilizes the Adaptive Halftoning [19] where in the dynamically determined threshold for halftoning, results in better contrast for both constantly varying images and sharp transition images. The human eye perceives the tiny dots as white and denser dots as black, in the halftoned image. A gray scale image and its halftoned image is shown in Fig. 2.

Fig. 2 a) Continous tone b) Halftone

Extended Visual Cryptography Scheme (EVCS)

The shares generated in the VCS bears a noise like image. Though, it may reveal no clue about the secret image, it may however raise suspicions about the secret. In order to overcome the weakness of noise like VCS shares, they are embedded with the individual cover images, thus generating the meaningful shares. The VCS with meaningful shares are referred as Extended Visual Cryptography Scheme (EVCS). The meaningful shares depict the cover image and not the secret image. However, on overlapping the meaningful shares, the secret image is decoded.

Color Visual Cryptography Scheme

Conventional VCS is applicable only for binary images. For grayscale image, it is to be halftoned to binary image as discussed in section II-B.

In the proposed scheme, adaptive halftoning is implemented. The color image is generally constituted by either subtractive or additive models as in Fig. 3.

Fig. 3 a) Subtractive model, and b) Additive model

In the subtractive model, with primary color components as cyan (C), magenta (M) and yellow (Y), the other colors can be obtained with proper mixing of CMY components. The color printer is based on subtractive model.

In additive model, the desired color is achieved from proper mixing different Red (R), Green (G) and Blue (B) color components. By mixing the RGB components of equal intensity, white color can be obtained. Computer monitor is based on additive model.

The secret color image can be decomposed into Red, Green and Blue frames. The individual frames will then be a gray pattern of the corresponding color components. These frames are adaptive halftoned to obtain the binary images which can be used for generation of shares in Red, Green and Blue components. By concatenating these RGB components of each shares, the corresponding color shares are obtained.

Overlapping the color shares, the color secret image is decoded.

Polynomial Image Secret Sharing Scheme (PISSS)

PISS scheme was first implemented [16] to hide a secret image. Though, it contradicts the advantage of VCS, by involving mathematical calculations in both encrypting and decrypting stages, it offers perfect retrieval of the

secret image pixels. The PISS is implemented for TiOISSS with perfect reconstruction [20].

The polynomial in equation 1, encodes the image pixels to cipher data, which is then embedded in GVCS shares.

in which are the sequential *k* pixels of the image and *P* is the prime number.

In the decoding phase, the Lagrange interpolation formula in equation (2) is used to derive the polynomial coefficients,

By substituting the pixel position for , where, , keeping as the variable, theA, A polynomial coefficients is derived, A, A Further, the decoding polynomial equation can be derived by from the polynomial coefficient and the encoded image pixels in equation (3).

The original secret pixel value can be retrieved from the equation (3), by substituting the image pixel position ,. A large prime number of 251, which is within the gray pixel range, can be considered for encrypting the grayscale image.

TiOISSS

Two in One Image Secret Sharing Scheme (TiOISSS) [18] combines the merits of both PISS to achieve perfect reconstruction & VCS to decode the vague secret image by HVS. Hence, it involves two levels of encoding and decoding phases.

The encoding phase starts with generating *n* VCS shares and *n* PISS shares from the same secret image, followed by replacing the black pixels of VCS

shares by the gray-valued pixels of PISS shares to generate GVCS shares, which are transmitted through n users. In the decoding phase, the GVCS shares from the users are overlapped to reconstruct the vague secret image, in the 1st stage level with just HVS. This process does not require any mathematical computations. Further, Inverse PISS is applied to the gray pixels of GVCS shares to perfectly retrieve the secret image, in the 2nd stage level of decoding.

III. A, A Proposed scheme

In existing TiOISSS [19], the noisy shares were generated, which make attract the intruders to create a fake shares to forge the legitimate user. In the proposed scheme, the existing TiOISSS is modified for color images. The meaningful color EVCS shares are generated by embedding a color authentication image. The RGB components of color secret image and the cover images are extracted as in Fig. 4. The modified TiOISSS is applied for each color components to generate the corresponding the color components of GVCS shares. By concatenating the RGB components, color GVCS shares are obtained.

The vague color secret image and the authentication image can be decoded, in the first decoding phase. Additionally, to provide additional authenticity, a 216 bits of textual message is embedded in the two LSBs of white pixels of all GVCS shares, which are then decoded in the 2nd phase. The RGB components of color secret image and the authentication image are then retrieved by applying Inverse PISS. The stages involved in the proposed

modified color TiOISSS with the generation of meaningful EVCS shares and including an authentication image are discussed in the following sections.

EVCS Share generation

EVCS shares are generated from the individual RGB components of the secret color image, authentication image and the cover image. The Left half of the secret image is considered for generating the left half of VCS shares (LS1 and LS2) as in Fig. 5. By considering the authentication image, the right half of VCS shares (RS1 and RS2) are generated.

For each RGB components of the secret image, the following steps are followed to generate the corresponding RGB components of the VCS shares.

1. From the left half of secret image (LS), the left half of share1 (LS1) and the left half of share2 (LS2) are generated.

2. For every black pixel of the halftoned authentication image, corresponding subpixels of left half of share 2 (LS2) with one pixel modified from white to black is placed in the corresponding subpixel location of right half of share 1 (RS1). Thus, the RS1 and LS2 will decode the vague authentication image.

3. For each black pixels of RS, the corresponding sub-pixels of the right half of share 1 (RS1) with modified location of black pixels is placed in the corresponding subpixel location of right half of share 2 (RS2).

4. VCS shares are obtained by combining the left half and the right half of each shares.

To overcome the weakness of noisy shares, cover images are embedded to generate the meaningful shares. Each RGB components of the VCS shares are processed as shown in Fig. 5, with the corresponding RGB components of the cover images. For every black pixel in each cover image component, the corresponding sub-pixel location of the respective VCS share component is modified such that one white pixel converted to black. The location of the converted black pixel depends on the pixel value of the secret image in the corresponding location. Thus, the EVCS shares components are generated from the VCS shares and the cover images.

GEVCS Share generation

The color secret image is first decomposed into RGB components and the pixels of each component are permuted in three levels to improve the security. In the proposed scheme, the 128 bit of encryption key is used as formatted in Fig. 6 is used to perform the permutation in bit level, block level and pixel level with respective 32-bit keys. The permutation order key defines the order of permutation performed which is required in reverse permutation operation. The GVCS share order defines the share order to be processed to retrieve the embedded key from the GVCS shares. The size of the textual secret message embedded in the GVCS shares is defined in the 16-bit Secret Message length.

The PISS shares are generated from the permuted color secret image as detailed in section II-E. The resultant PISS values and the authentication color image pixels are embedded into the black sub-pixels are the EVCS shares. Prior to embedding these PISS values, it is truncated by a factor

AZA± , (*AZA±* = 1, 2, A? a,¬A¦ 16). This truncated value along with its remainder in GEVCS shares will be darker near to black, providing better visual quality. Thus, the truncated permuted PISS values, the color authenticated image and the textual secret message are embedded into EVCS shares to generate the GEVCS shares as detailed in the Fig. 7.

Decryption of the Secret image

The decoding of the secret image is done in two phases. In the first phase, the two GEVCS shares are overlapped to decode the vague color secret image. To verify its authenticity, RS1 and LS2 of the GEVCS shares are superimposed to decode the authentication image.

In the second phase of decoding, the encryption keys and the secret messages are extracted from the white pixels of each GEVCS shares. The PISS values are retrieved from the GEVCS shares. Inverse PISS is applied to reconstruct the secret image and the authentication image are perfectly. The process is explained in Fig. 8.

IV. A, A Experimental Results

The experimental results of the proposed Authenticated Color Extended TiOISSS with perfect reconstruction are discussed in this section. This scheme is implemented for truncation factor, AZA± = 7 and adaptive halftoning technique is applied for VCS share generation.

The 256? 256 sized color secret image and the 256? 128 sized color authentication image are considered as shown in Fig. 9(a) & 9(b). The color cover images of 256? 256 size are shown in Fig. 9(c) & 9(d). The Adaptive

halftoning version of the secret image and cover images are shown in Fig. 9 (e), 9(f) & 9 (g). Applying VCS over the halftoned authentication and the secret image with pixel expansion, m = 4, two VCS shares of 512? 512 are generated and is shown in Fig. 9 (h) & 9 (i). The GVCS shares generated from VCS shares by embedding PISS values as detailed in section III-B are shown in Fig. 9 (j) & 9 (k).

In the first level of decoding, the two GEVCS shares are overlapped to decode the vague color secret image. To verify the authenticity, LS2 and RS1 are overlapped to reveal the vague authentication image. They are shown in Fig. 9 (l) & 9 (m). In the 2nd decoding phase, by applying Inverse PISS and reverse permutation over the extracted gray pixels of the GEVCS shares, the perfect reconstruction of both the color authentication image and the color secret image is decoded as shown in Fig. 9 (n) & 9 (o).

V. Quality Analysis

The parameters like Contrast, Structural Similarity Index Measure (SSIM) & Peak Signal to Noise Ratio (PSNR) of the Authenticated Color Extended TiOISSS are analysed.

Contrast

Contrast which represents the visual quality of the image, is given by the normalized difference between the mean grayness of the white secret pixels and the mean grayness of black secret pixels in the decoded image. A, A In this scheme, contrast [20] is calculated among the group of decoded pixels

valued more than the threshold, (*C 0*) and the group of decoded pixels valued lesser than the threshold, (*C 1*) and is given by,

Contrast between the color secret image and its 1st decoded secret image for adaptive halftoning technique and between the authentication image and its 1st decoded output has been tabled in Table I for various truncation factor, AZA±. The contrast is improved

SSIM

It is a measure of resemblance between two images and it is calculated for two common sized (*N* A?- *N)* windows x and yof the two images. SSIM is given by

where

and are the average of *y* and *x.*

A, A and are the variance of *x* and *y* , is the covariance of *x* and *y*

and are two variables to stabilize the division, *L* is the dynamic range of the pixel values andA, A and by default.

The SSIM between the color secret image and its 1st decoded secret image for adaptive halftoning technique and between the authentication image and its 1st decoded output has been tabled in Table I for various truncation factor, AZA±. The SSIM is improved resulting in increased similarity between the secret image and the decoded secret image.

PSNR

The Peak Signal to Noise Ratio (PSNR) is a measure to estimate the image quality between two images. Based on the pixel difference between the reconstructed image and the original image, PSNR is defined as

where *MSE* denotes Mean Squared Error and $s = 255$, the maximum pixel value of the image.

The PSNR between the color secret image and its 1st decoded secret image for adaptive halftoning technique and between the authentication image and its 1st decoded output has been tabled in Table I for various truncation factor, AZA±. The PSNR is higher for lesser value of the truncation factor.

TABLE I

Comparison of Secret Image andA, A 1ST PHASE DECODED Secret Image

Secret image vs Decoded Secret image (1st phase)

Auth image vs Decoded Auth image (1st phase)

AZA±

Contrast

SSIM

PSNR

Contrast

SSIM

PSNR

1

Not possible, No Truncation

Not possible, No Truncation

2

0. 1324

0. 2556

3

0. 1314

0. 2446

6. 7766

0. 1720

0. 1260

4. 3907

4

0. 1330

0. 2452

6. 5423

0. 1708

0. 1498

4. 1201

5

0. 1322

0. 2380

6. 5246

0. 1762

0. 1769

4. 1499

6

0. 1319

0. 2352

6. 4209

0. 1752

0. 1950

4. 0422

7

0. 1318

0. 2328

6. 3584

0. 1753

0. 2082

3. 9912

8

0. 1325

0. 2348

6. 3265

0. 1746

0. 2217

3. 9447

9

0. 1320

0. 2322

6. 3640

0. 1772

0. 2277

4. 0184

10

0. 1317

0. 2316

6. 3082

0. 1771

0. 2351

3. 9738

11

0. 1313

0. 2292

6. 3050

0. 1761

0. 2378

3. 9582

12

0. 1312

0. 2291

6. 2671

0. 1768

0. 2444

3. 9383

13

0. 1311

0. 2307

6. 2571

0. 1765

0. 2476

3. 9250

14

0. 1307

0. 2286

6. 2791

0. 1750

0. 2436

3. 9232

15

0. 1302

0. 2280

6. 2373

0. 1760

0. 2510

3. 8964

16

0. 1312

0. 2322

6. 2348

0. 1751

0. 2528

3. 8830

Table II shows the comparison of meaningful shares with the corresponding cover images, which depicts that meaningful shares offers better visual quality.

TABLE II

Parameter Comparison for GVCS Shares vs Cover Images, for AZA± = 7

Proposed Scheme

GEVCS 1

GEVCS 2

Contrast

0. 1239

0. 1746

SSIM

0. 2803

0. 1807

PSNR (dB)

6. 1746

6. 2839

Table III shows the comparison of different halftoning techniques, which shows that the adaptive halftoning offers better visual quality.

TABLE III

Parameter Comparison between the Secret Image and 1st decoded Secret Image, for Different Halftoning, for AZA± = 7

Halftoning Technique

AM Halftoning

FM Halftoning

Adaptive Halftoning

% Improvement

FM vs Adaptive

Contrast

0. 0947

0. 0988

0. 1318

33. 40

SSIM

0. 0755

0. 1823

0. 2328

27. 70

PSNR (dB)

6. 1453

6. 2268

6. 3265

1. 60

VI. Security Analysis

The security of the proposed scheme is discussed here with the following security aspects.

Authentication image for additional security

With any one of the GEVCS color shares, the hackers may generate the other counterfeit shares, such that the legitimate receiver may get a bogus secret image instead of the original secret image. To overcome this weakness, a color authentication image is encoded into the GEVCS shares. In the 1st level of decoding, the vague authentication image is reconstructed and is used to

validate the genuineness of the secret image, thus enhancing the security of the scheme. Further, the perfect retrieval of the authentication image is achieved by computations, in the 2nd decoding phase.

Histogram of Shares

Fig. 10 shows the histogram pattern of the color GEVCS share 1, for truncation factor AZA± = 7. It can be observed that the pixels occupy value up to 36 (i. e. 28/AZA±) and at 255. By choosing different values of AZA±, the pixel distribution of GEVCS shares can be limited accordingly. Unlike the original secret image, where pixels are distributed over the entire range, GEVCS shares are secured with limited pixel distribution, thus enhancing the security of the proposed scheme.

Fig 10: The Histogram pattern of GEVCS shares1, (AZA± = 7)

VII. Conclusion

The proposed Authenticated Color Extended Visual Cryptography with perfect reconstruction overcomes the disadvantages of conventional TiOISSS with the implementation of color cover images in GEVCS shares. In the proposed scheme, the color secret image is permuted in three stages viz. bit level, pixel level and block level, and PISS algorithm is implemented for perfect decoding of the secret image. Additionally, an authentication color image and a textual secret message is encoded in GEVCS shares to authorize the validity of the decoded secret image. Adaptive Halftoning improves the contrast of the 1st level decoded secret image. Quality parameters like SSIM, PSNR and Contrast have been improved and Security

have been enhanced with the use of the Authentication image and the 128-bit Encryption key for the generation of color meaningful shares from the cover images.

References

M. Naor and A. Shamir, “ Visual Cryptography”, Alfredo De Santis (Ed.), *Advances in Cryptology Proceedings of Eurocypto 94* , Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1994. M. Naor, A. Shamir, in: M. Lomas (Ed.), Visual Cryptography, II: “ Improving the Contrast via the Cover Base” Presented at *Security in Communication Networks* , Amalfi, Italy, September 16-17, 1996. G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, “ Visual cryptography for general access structures”, *Inform. Comput* . 129 (1996) 86-106. S. Arumugam, R. Lakshmanan and Atulya K. Nagar, “ On (k, n) visual cryptography scheme”, *Journal of Designs, Codes and Cryptography* , vol. 71, no. 1, pp. 153-162, July 2014R. W. Floyd and L. Steinberg, “ An adaptive algorithm for spatial grayscale”, *Proc. SID* , 17/2: 75-77, 1975C. Blundo, A. De Santis, M. Naor, “ Visual cryptography for grey level images”, *Inf. Process. Lett* . 75 (2000) 255-259. C. C. Lin, W.-H. Tsai, “ Visual cryptography for grey-level images by dithering techniques”, *Pattern Recognition* Lett. 24 (2003) 349-358. Nakajima, M. and Yamaguchi, Y., “ Extended visual cryptography for natural images”, *Journal of WSCG* , v10 i2. 303-310. G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, “ Extended capabilities for visual cryptography”, *Theor. Comput. Sci. 250* (2001) 143-161V. Rijmen, B. Preneel, “ Efficient colour visual encryption for shared colors of Benetton”, *Eurocrypto’96* , Rump Session, Berlin, 1996. Y. C. Hou, “ Visual cryptography for color images”, *Pattern Recognition* 36 (2003) 1619-1629. Y. C. Hou, F.

Lin, C. Y. Chang, “ Improvement and implementation of the secret color image sharing technique”, *Proceedings of the Fifth Conference on Information Management* , Taipei, November 1999, pp. 592-597. Y. C. Hou, F. Lin, C. Y. Chang, “ A new approach on 256 color secret image sharing technique”, *MIS Review* , No. 9, December 1999, pp. 89-105. Y. C. Hou, C. Y. Chang, F. Lin, “ Visual cryptography for color images based on color decomposition”, *Proceedings of the Fifth Conference on Information Management* , Taipei, November 1999, pp. 584-591. Der-Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, Chwei-Shyong Tsai, “ A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares”, *Journal of Displays, Elsevier* , vol. 32, pp. 118-134, 2011. Chih-Ching Thien and Ja-Chen Lin, “ Secret image sharing”, *Journal of Computers & Graphics* , vol. 26, no. 5, pp. 765-770, October 2002. Sian-Jheng Lin and Ja-Chen Lin, “ VCPSS: A two-in-one two-decoding options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches”, *Journal of Pattern Recognition Letters* , vol. 40, no. 12, pp. 3652-3666, April 2007. Peng Lia, Pei-Jun Maa, Xiao-Hong Sua and Ching-Nung Yang, “ Improvements of a two-in-one image secret sharing scheme based on gray mixing model”, *Journal of Visual Communication and Image Representation* , vol. 23, no. 3, pp. 441-453, January 2012. Srividhya Sridhar, R. Sathishkumar, Gnanou Florence Sudha, “ Adaptive halftoned visual cryptography with improved quality and security”, *Journal of Multimedia Tools and Applications* , pp. 1-20, November 2015. S. Srividhya, R. Sathishkumar, Gnanou Florence Sudha, “ Implementation of TiOISSS with meaningful shadows and with an additional authentication Image”, *Journal of*

Visual Communication and Image Representation , vol. 38, pp. 284-296, July 2016.