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 2, February 2017

Extended Digital Image Sharing by Disparate Image Media with Hoaxer Detection

Anna Joseph

M.Tech, Dept. of CSE, Viswajyothi College of Engg. & Technology, Vazhakulam P. O, Kerala, India

ABSTRACT: At present, customary Visual Secret Sharing (VSS) strategies undergo transmission risk challenges for the secret itself and for the participants who are involved in the VSS technique environment. To address this challenge, a natural-image-based VSS (NVSS) strategy that shares secret images via disparate image media to protect the secret and the participants during the transmission phase is proposed. Here, the proposed (*n*, *n*) – NVSS scheme can share one digital secret image and one noise-like share. The secret image is shared over *n* - 1 arbitrary selected natural images or natural shares. Other than natural shares, digital images can also be used in the secret sharing method. A dishonest or malicious participant called hoaxer can provide Fake Share (FS) to cheat the other participants which is possible in Visual Cryptographic Schemes (VCS). To achieve hoaxer detection in VCS a secret message (key) is embedded in the random locations of each of the shares during share generation phase. Thus, in this method the noise-like share is generated based on the natural shares, secret image and secret key.Lazy Lifting Wavelet Transform is used to hide the noise-like share to reduce the transmission risk challenges for the share. The unaltered natural shares are disparate, thus greatly reducing the transmission risk challenges.

KEYWORDS*:* Visual secret sharing scheme, visual cryptography, natural shares, steganography, transmission risk, fake share

I. INTRODUCTION

Nowadays, digital images are seen everywhere. At least once in our daily life we come across a digital image in one way or the other. Either it can be in smartphones or laptops. The range of using digital images is from our cellphones to pages and websites available online. Therefore, it is crystal clear that digital images have become a part of our day-to-day life. Technology is growing everyday making everything at our finger tips, just a click away. Highly sophisticated machines and advanced systems are developed and deployed with a high degree of skill and knowledge. So the faster we move with enhancements and better techniques for secure and confidential environment

In visual cryptography (VC), a secret image is encrypted and split into *n* shares depending upon the number of participants. Anyone who holds lesser than *n* shares cannot reveal any information regarding the secret image. Stacking the *n* shares reveals the secret image and it can be grasped directly by the human visual system. Secret images can be of varied types: images, handwritten documents, photographs, and others. Sharing and delivering secret images are also known as a visual secret sharing (VSS) scheme. The basic principle of VC was first introduced by Noar and Shamir [1].

Steganography otherwise known as information hiding focuses on hiding secret images without a trace of its existence. Usually, the hiding of confidential or secret data is done in benign image shares. This helps to conceal the actuality of the secret data which must be kept behind the scenes. Steganographic mechanisms are used in embedding secret data both in textual or image formats.

In this system, to minimize the transmission challenges natural-image-based VSS (NVSS) strategy is adopted. Conventional VSS schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form [1]. The shares can be: noise-like pixels or meaningful images. The natural shares can be: digital and printed images, landscape and portrait photographs, hand-painted pictures, flysheets and so on. NVSS scheme uses disparate image media which provides a platform for securely sharing secret images. Applying a diversity of media for sharing the secret image increases the degree of difficulty of intercepting the shares [1]. The proposed NVSS strategy can share a digital secret image over *n* -1 arbitrary natural image and one noise-like share. Instead of rearranging the pixel contents of the natural images, the proposed approach extracts features from each digital or natural share. The chance for the introduction of fake shares (FS) is extremely inevitable. A hoaxer (dishonest or malicious participant) can provide FS without the knowledge of other participants thereby cheating the honest participants. For hoaxer detection, a secret numerical message is embedded during noise-like share generation. The generated share that is noise-like can be hidden by using steganographic mechanism to maximize the security level during the transmission aspect. The unaltered natural shares are totally benign, thus greatly reducing the interception probability of the shares.

The remainder of this paper is organized in this manner: Section II contains the details of the related papers. Section III describes the proposed system model's overview and Section IV gives the implementation methodologies. A detail of experimental work is explained in Section V. Section VI includes conclusion and suggestions for future work.

II. RELATED WORKS

In the paper, the major algorithms like (*n*, *n*)-NVSS encryption/decryption and feature extraction are adopted from [1]. Therefore this work is an enhancement of the base paper [1]. Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents [6], [7], but they suffer from two drawbacks: first, there is a high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be intercepted. Thus, the risk to both the participants and the shares increases, in turn increasing the probability of transmission failure. Second, the meaningless shares are not user friendly. As the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares.

Previous research into the Extended Visual Cryptography is photos or hand-painted pictures in digital form or in printed Scheme (EVCS) or the user friendly VSS scheme provided some effective solutions to cope with the management issue [4], [5] and [8]. The shares contain many noise-like pixels or display low quality images. Such shares are easy to detect by the naked eye, and participants who transmit the share can easily lead to suspicion by others. Existing research focuses only on using transparencies or digital media as carriers for a VSS scheme. The transparency shares have either a noise-like or a meaningful appearance. The conventional noise-like shares are not friendly [6] and [7]; hence, researchers tried to enhance the friendliness of VSS schemes for participants [8].The XOR-based VC is a possible methodology to solve the poor visual quality problem without darkening the background in VC [9].

III. SYSTEM OVERVIEW

A. BACKGROUND

For secure communication, the one-time pad (OTP) available in cryptography was proven to be impossible to break if used exactly, was developed by Gilbert Vernam in 1917. Each bit or character from the plaintext is encoded by a logical XOR operation with a bit or character from a secret random key of the same length as the plaintext that outcomes cipher text. The cipher text was sent to a receiver then; the original plaintext can be decrypted in the receiver side by applying the same operation and the same secret key as the sender used for encrypting the cipher text [1].

In a (2, 2) - VSS scheme [1], the secret random key and the cipher text that can be treated as two shares in the scheme were distributed to two participants who involve in the scheme. The two participants can decode the secret by applying the decryption operation to the shares that were held by the participants. The idea of the OTP technique to share digital visual secrets is used here. The following assumptions [1] are made:

1. When the number of delivered shares increases, the transmission risk also increases.
2. The transmission risk of shares with a meaningful cover image is less than that of noise-like shares.
3. The transmission risk decreases as the quality of the meaningful shares increases.
4. The natural images without artificially altered or modified contents have the lowest transmission risk, lower than that of noise-like and meaningful shares.
5. The display quality of distortion-free true color images is superior to that of halftone images**.**

B. (N, N)-NVSS METHODOLOGY

Fig.1 shows the encryption process of the (*n, n*) - NVSS scheme where *n*≥ 2. It includes three main phases: feature extraction, encryption and hide noise-like share.(*n, n*) - NVSS scheme can encipher a true color secret image by *n* - 1 innocuous natural shares and one noise-like share.

In the feature extraction phase, binary feature images are extracted from each natural as well as digital share. Subsequently, the feature images extracted are combined to make one feature image with 24-bit/pixel color depth.

In the encryption phase, the *n* - 1 feature images and the secret image execute the XOR operation along with secret key to generate one noise-like share S with 24-bit/pixel color depth.

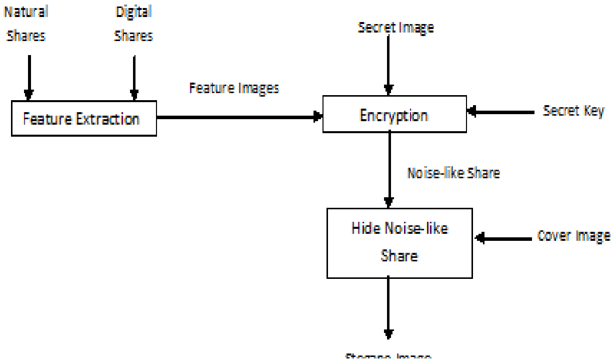


Fig.1 Encryption process of the (*n, n*)-NVSS methodology

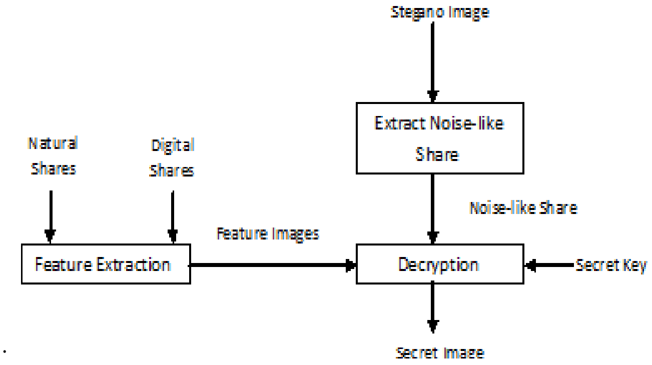


Fig. 2 Decryption process of the (*n, n*)-NVSS methodology.

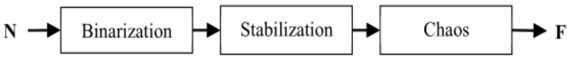


Fig. 3 Block diagram of Feature Extraction

Then, to reduce the transmission risk challenge of noise-like share, it is concealed behind cover media by Lazy Lifting Wavelet transform [3]. The resultant share S' is called the generated share. The *n* - 1 benign natural and digital shares along with the generated share are *n* shares in the (*n, n*)-NVSS scheme.

In the decryption phase, when all *n* shares are received, extraction of *n* - 1 feature images from all natural and digital shares is done and then executes the XOR operation with share S' and compare with the secret key to obtain the recovered image, as shown in Fig. 2.

IV. IMPLEMENTATION DETAILS

This section gives the detailed technical description like algorithms, images, mathematical equations and other implementation parameters.

Extended Digital Image Sharing by Disparate Image Media with Hoaxer Detection belongs to the area of image processing. The famous computing environment favorable for image processing is MATLAB. The complete implementation of the system is done using MATLAB R2014a.

A. Modules

Extended Digital Image Sharing by Disparate Image Media with Hoaxer Detection contains 2 dominant modules:

1. Encryption Module
2. Decryption Module

For the detailed view of system implementation, the major modules are further classified in the following way.

1) Encryption module

The significant algorithms used in encryption phase are feature extraction algorithm,(*n*, *n*) - NVSS encryption/decryption algorithm and key hiding algorithm. Lazy Lifting Wavelet transform is used to convert noise-like share to digital image. The following notations [1] are used in the paper:

- b represents the block size, b ∈ even.
- N denote images.
- (x, y) denotes the coordinates of pixels in the image shares and the secret image, $1 \leq x \leq w$, $1 \leq y \leq h$ where w and h are width and height of image respectively.
- (x_1, y_1) represents the coordinates of the left-top pixel in each block.
- Pixel value $H^{x,y}$is the sum of RGB color values of pixel (x, y) in N

$$H^{x,y}= p_R{}^{x,y}+ p_G{}^{x,y}+ p_B{}^{x,y}(1)$$

- M represents the median of all pixel values $(H^{x_1,y_1}, \ldots , H^{x_b,y_b})$ in a block of N.
- F is the feature matrix of N, the element $f^{x,y} \in F$denotes the feature value of pixel (x, y). If the feature value $f^{x,y}$ is 0, the feature of pixel (x, y) in N is defined as black.If $f^{x,y}$is 1 the feature of pixel (x, y)in N is defined as white.
- φ denotes a color plane of an image, $\varphi \in \{R,G,B\}$.
- S is the input image; $S\varphi$ denotes an element of S in color plane φ.
- $\bar{S}$ is the output image; $\bar{S}_\varphi$denotes an element of $\bar{S}$ in color plane φ.
- FI_αdenotes a feature image of share N_α.
- $FI_{\alpha,\varphi}$denotes an element of feature images in color plane φ.
- þ denotes the pixel value of $FI_{\alpha,\varphi}$ at coordinates (x, y), $0 \leq$ þ ≤ 255.

a) Share Generation

Share generation is the prime part of the system as it outputs the noise-like share after applying the feature extraction (Algorithm 1 [1]) and the (*n*, *n*) NVSS encryption/decryption algorithm (Algorithm 2 [1]). Noise-like share is extracted from the input natural images, secret image and secret key.

Feature Extraction: The section describes the feature extraction module [1] that extracts feature images from the input image shares. The module which is the core module of the feature extraction process is applicable to printed and digital images respectively. Here, the traditional wavelet transform is not applied to extract the feature images as the extracted feature image may contain some texture of the original image. This reduces randomness in the noise-like share and hence eliminates the security constraints. The proposed feature extraction algorithm removes the drawback of conventional methods. The feature matrix depends on the contents of the corresponding natural/digital image rather than the secret image [1]. Fig. 3 shows the block diagram [1].

By the process of binarization, a binary feature matrix is obtained from each input image. The binary feature value of each pixel is obtained by Eq. (2). As in [1], to obtain an approximate appearance probability for binary values

0 and 1, the median value M of pixels in the same block is an obvious selection as the threshold. Hence, for each block, the extraction function of pixel (*x*, *y*) of N (input images) is defined as follows:

$$f^{x,y} = F(H^{x,y}) = \begin{cases} 1, & H^{x,y} \geq M \\ 0, & \text{otherwise} \end{cases} \qquad (2)$$

By the process of stabilization, we can balance the number of black and white pixels of an extracted feature image in each block. The number of unbalanced black feature pixels Q_s calculated as:

$$Q_s = \left(\sum_{\substack{\forall x_1 \leq x \leq x_b \\ \forall y_1 \leq y \leq y_b}} f^{x,y} \right) - \frac{b^2}{2} \quad (3)$$

By the process of chaos, the texture that may appear on the extracted feature images and the noise-like share are eliminated by randomly selecting black feature pixels Q_c as in Eq. (4). P_{noise} be the probability to add noise in the feature matrix.

$$Q_c = \frac{b^2}{2} \times P_{noise} \qquad (4)$$

(n, n) - NVSS Encryption/Decryption: In [1], the proposed Algorithm 2 has some properties. The amount of information required for the generated share is the same as for the secret image and the pixel values in a feature image are distributed uniformly over [0, 255]. The pixel distribution has high randomness.

```
Algorithm 1: Feature Extraction (FE)
Input: N, b, $P_{noise}$
Output: F
    1.  Divide N into blocks with b × b pixels
    2.  For each block repeat Steps 3-11
    3.  $\forall x_1 \leq x \leq x_b, \forall y_1 \leq y \leq y_b$, calculate $H^{x,y}$ by Eq.(1)
    4.  Calculate M
    5.  $\forall x_1 \leq x \leq x_b, \forall y_1 \leq y \leq y_b$, determine $f^{x,y}$ by Eq.(2)
    6.  Calculate $Q_s$ by Eq.(3)
    7.  Randomly select $Q_s$ pixels where $f^{x,y} = 1$ and $H^{x,y} = M$, let $f^{x,y} \leftarrow 0$
    8.  Calculate $Q_c$ by Eq.(4)
    9.  Randomly select $Q_c$ candidate pixels where $f^{x,y} = 1$
    10. Randomly select $Q_c$ candidate pixels where $f^{x,y} = 0$
    11. Alter all values of $f^{x,y}$ that were selected in Steps 9 and 10
    12. Output F
```

```
Algorithm 2: (n, n) - NVSS Encryption/Decryption
Input: S, $N_1, \ldots, N_{n-1}$, b, $P_{noise}$
Output: $\bar{S}$
    1.  $n \leftarrow n_p + n_d + 1$
    2.  $\forall 1 \leq \alpha \leq n, \forall \varphi \in \{R, G, B\}, FI_{\alpha,\varphi} \leftarrow 0$
    3.  $\forall 1 \leq \alpha \leq n, \forall \varphi \in \{R, G, B\}, \forall 0 \leq i \leq 7$, repeat Steps 5 and 6
```

```
4.  Call procedure FE ($N_\alpha$, b, $P_{noise}$)
5.  $\forall(x, y)$, x ∈ [1, w], y∈ [1, h], $þ \leftarrow þ + f^{x,y} \times 2^i$
6.  Extract the feature value from the secret
    image using the RGB channel
7.  $\forall\varphi \in \{R, G, B\}$, $\bar{S}\varphi \leftarrow S\varphi \oplus FI_{1,\varphi} \oplus \ldots$
    $\oplus FI_{n-1,\varphi}$
8.  Output $\bar{S}$
```

b) Key Hiding

In Extended Digital Image Sharing by Disparate Image Media with Hoaxer Detection, the number of shares is fixed. Cheating is possible by dishonest or malicious participant called a hoaxer or cheater. This is done by replacing the original shares with Fake Shares (FS) to cheat the other honest participants. There are two types of hoaxers in this scenario. One is a malicious participant who is also a legitimate participant, and the other is a malicious outsider [2].

```
Algorithm 3: Key Hiding
    1.  Consider the shares and the secret image
    2.  Using pseudo random generator, create some
        random location in the shares
    3.  Save the locations
    4.  Then embed the secret key into the random
        location of share images
    5.  Finally get the noise-like share
```

To check the originality of the share, check whether the secret key is present on that share or not. To recognize the fake shares, collect all the shares from the participants, then check the secret key embedded within each shares before stacking, if the message is intact then that is the original share otherwise it is fake share which can detect possible cheating in VCS by validation [2]. Algorithm 3 shows the steps of key hiding.

c) Noise-like Share to Digital

Noise-like shares always arouse suspicion and increase interception risk during transmission of shares. Here, in order to eliminate this situation noise-like share is converted to digital meaningful share with the help of a cover image. Use the Lazy Lifting Scheme [3] by applying an Integer Wavelet Transform. The lifting scheme calculates wavelet transforms in an efficient way, and can easily be converted to an integer transform. This can be done easily by adding some rounding operators.

2) Decryption module:

The significant algorithms used in decryption phase are feature extraction algorithm,(*n*, *n*) - NVSS encryption/decryption algorithm and extraction secret message algorithm. Inverse of lazy lifting wavelet transform is used to extract noise-like share from the cover digital image.

a) Noise-like Share Extraction

In the previous section of encryption phase the noise-like share is converted to a digital meaningful share by using Lazy Lifting Scheme. At the beginning of decryption phase, it is necessary to extract the noise-like share from the cover image and thereby extracting the secret image. To retrieve the noise-like share applies the inverse of Lazy Lifting Wavelet Transform [3].

b) Key Extraction

To check whether any fake share is included (by replacing original share) in the decryption phase the hidden key must be extracted from the shares (use Algorithm4), then compare it with the input key to find out the fake share (if any).

```
Algorithm 4: Key Extraction
    1. Consider the input shares and noise-like share
    2. Get the random locations
    3. Input the secret key:
        3.1 If secret key is correct, then the secret image is retrieved
        3.2 If secret key is correct and any of the share is fake, then secret image is not retrieved
        3.3 If secret key is wrong, then "KEY MISMATCH" and secret image is not retrieved
```

If the input key and extracted key matches the shares in decryption phase are original, otherwise fake shares (one or more) included by the hoaxer [2]. Algorithm 4 is used to extract the secret key from shares.

c) Information Extraction

Here, the (*n, n*) -NVSS encryption/decryption [1] scheme is applied to extract the secret image. This is done by providing the input natural or digital shares and secret key. From Algorithm 4, steps 3.1 to 3.3 gives procedure for information extraction.

V. EXPERIMENTS

This section performs experiments to evaluate the performance of the proposed system. Hence, to prove that Extended Digital Image Sharing by Disparate Image Media with Hoaxer Detection is the better solution to reduce the transmission risk challenges.

The input image shares contain both digital and natural shares. The natural images are captured using different cameras of smartphones, tablets and webcams. The devices include iPhone 6, Samsung Techwin/Tab, HP Pavilion dm4, Lenovo S660, Sony DSC-W350, Nokia 5230/5800 and Motorola XT1068. The following considerations are made to experiment on the system:

- (6, 6)-NVSS Encryption/Decryption Scheme is used i.e. 5 natural or digital image shares and 1 secret image
- PSNR (peak signal to noise ratio) is calculated.

The low PSNR means that high distortions are introduced into the digitized share that will be used in the decryption phase of the system. The distortions introduced might be due to the various devices used for capturing the natural image shares during the encryption/decryption phases [1].

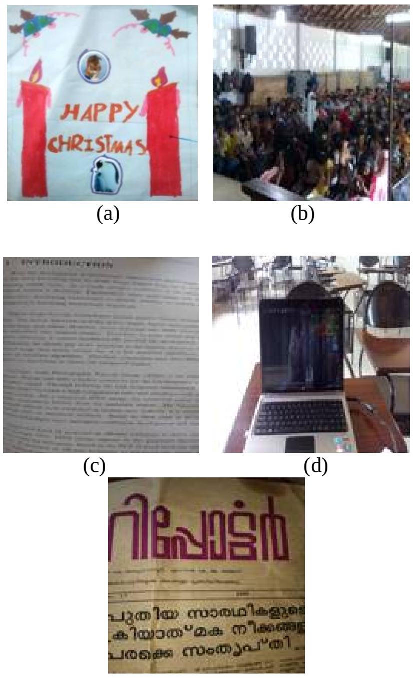
Table 1. PSNR value of Proposed System using (6, 6)-NVSS Encryption/Decryption

Sl. No.	No. of Digital Shares	No. of Natural Shares	No. of Secret Image	PSNR
1	4	1	1	38.4575
2	3	2	1	38.4495
3	2	3	1	38.1601
4	1	4	1	38.0522
5	Nil	5	1	38.6691

PSNR value for the system is calculated between the provided secret images and retrieved secret image. Since the system use disparate images, digital image shares as well as natural image shares can be given as input to the system. In the Table I, the second column represents the number of digital image shares, for example Lena. The third column denotes the natural image shares like printed images, landscape and portrait photographs, hand-painted pictures, flysheets and so on. The fourth column shows the PSNR values of the proposed systems.

In Table 1, the first input to the system is 4 digital shares, 1 natural share and 1 secret image. In the further evaluation phase, the number of digital image shares is decreased while the number of natural shares is increased. Even in the last case only natural image shares are present. Then also the proposed system results in a better PSNR value i. e. 38.6691.Hence, the proposed system is a good solution to reduce transmission threats.

Fig. 4(a) is a scanned image, rest of the images Fig. 4(b)-(e) are captured using iPhone 6, Motorola XT1068, Lenovo S660 and Samsung Galaxy Tab 10 respectively. In Fig. 5, the input secret image Fig. 5(a) is from [1] and the resultant image after decryption has only less noise pixels. Fig. 5(b)-(c) are the output from the system. Hence, the proposed system is a good solution to reduce transmission threats.

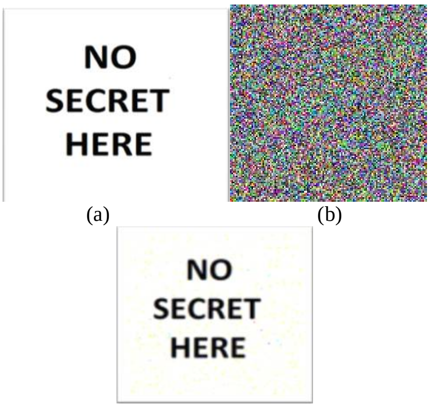


(a) (b)

(c) (d)

(e)

Fig. 4 (a)-(e) Natural image shares used in (6, 6)-NVSS encryption/decryption scheme



(a) (b)

(c)

Fig. 5 (a) Input secret image, (b) noise-like share, (c) resultant image after decryption (PSNR=38.6691)

VI. CONCLUSION AND FUTURE ENHANCEMENTS

Extended Digital Image by Disparate Image Media with Hoaxer Detection deployed (*n, n*)-NVSS encryption/decryption scheme that can share a digital image using disparate image media. It includes *n* - 1 randomly chosen images (which can be natural or digital) and one secret image in the encryption phase. Apart from that encryption phase, it also embed a secret key in shares (including noise-like share) and using steganographic mechanism, noise-like share is converted to a meaningful share by adding a cover image. Therefore, they are totally benign. Regardless of the number of participant's *n* increases, the NVSS scheme uses only one noise share for sharing the secret image. Hence, the proposed encryption/decryption strategy can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants.

Here, the number of share is fixed and input secret image is black and white. Hoaxer detection is done but no special strategy for prevention. As a future enhancement, hoaxer prevention can be done, use of colour images can be enabled and number of shares can be made dynamic.

VII. ACKNOWLEDGEMENTS

First of all I thank the Father Almighty for the immense graces and blessings showered upon me. Then I extend my sincere and heartfelt gratitude to all the important personalities who have helped me throughout the development and implementation of this project work.

REFERENCES

1. K. H. Lee and P. L. Chiu, 'Digital Image Sharing by Diverse Image Media', IEEE Trans. Inf. Forensics and Security, vol. 9, no. 1, Jan 2014.
2. B. Jana, P. Chowdhuri, M. Mallick and S. K. Mondal, 'Cheating Prevention in Visual Cryptographic using Steganographic System', International Conference on Issues and Challenges in Intelligent Computing Techniques, 2014.
3. K. Patel, K. K. Rora, K. Singh and S. Verma, 'Lazy Wavelet Transform Based Steganography in Video', International Conference on Communication Systems and Network Technologies, 2013.
4. Kang, G. R Arce and H. Lee, 'Color Extended Visual Cryptography Using Error Diffusion', IEEE Trans. Image Processing, vol. 20, no.1, Jan 2011.
5. F. Liu and C. Wu, 'Embedded Extended Visual Cryptography Schemes', IEEE Trans. Inf. Forensics and Security, vol. 6, no. 2, June 2011.
6. P. L. Chiu and K. H. Lee, 'A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes', IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 9921001, Sep. 2011.
7. K. H. Lee and P. L. Chiu, 'Image Size Invariant Visual Cryptography for General Access Structures Subject to Display Quality Constraints', IEEE Trans. Image Process., vol. 22, no. 10, pp. 38303841, Oct. 2013.
8. K. H. Lee and P. L. Chiu, 'An Extended Visual Cryptography Algorithm for General Access Structures', IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219229, Feb. 2012.
9. X. Wu and W. Sun, 'Extended Capabilities for XOR Based Visual Cryptography', IEEE Trans. Inf. Forensics and Security, vol. 9, no. 10, Oct. 2014.

BIOGRAPHY

Miss. Anna Joseph has done her B.Tech and M.Tech in Computer Science & Engineering from Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala. The college is affiliated to M. G University. Her research interests are Image Processing, Network Security and Mobile Security.