Image Security using Digital Image Watermarking and Visual Cryptography Techniques

B. Jagadeesh, K. L. Sivan Prasad Reddy

Abstract: ***In today's world, the enhancement in internet technologies, digital data are mostly used to share the information in public networks. There are many traditional security techniques used to provide security to the digital information. But the existing methods don't provide much of the security to digital media like image, video, audio, etc. The digital watermarking is employed in the protection of digital information. This paper gives a review on digital image watermarking based on the visual cryptography to reach secure protection for the images. The secret information can be inserted in the original images. The secret key is generated from the watermark image with the help of visual cryptography to claim the ownership of images. Various types of Visual Cryptography and Digital Image Watermarking techniques are explained in real time application.***

Keywords: Digital image watermarking, visual cryptography, image security, encryption and decryption, copyright protection

I. INTRODUCTION

In the present era, the uses communication devices and technologies are increasing day by day. The digital information is most used digital data formats in computer networks for sharing between the different nodes. The digital data can be shared and accessed throughout the open network, and it is easy to access by everyone who has a network facility. The unauthorized people can access the content from the source and they change the content of the original information. In this, the data can losses its originality. The digital watermarking plays the main key role in avoiding security issues in open networks. In watermarking technique, the watermarks like the information about the owner's logo, secret, data, and symbol can be inserted in other data. The way of embedding the watermark can be done in two domains. It can be spatial domain or transform domain. The watermarks are inserted in the visible or invisible form. The two domains are spatial domain and transform domain.

In the spatial domain, the content of the watermark can be inserted in other data by change content of cover data. The digital image watermarking is used for protecting the copyright.

The paper is organized as follows: Section 2 provides a literature review, section 3 gives the necessity of data security, section 4. Overview of visual cryptography-based watermarking and section 5 and at least gives conclude the paper.

II. EXISTING METHODS

Ms. Priyanka Ramesh Shirsat et al. [1] and T. Sowmya, et al. [2] implemented a method to provide copyright protection for digital images. Here, the watermark can be split into two shares using visual cryptography. The DWT-SVD transforms are used to embed the shares on the host image and the watermark can be recovered by superimposing both pubis1 and pubis 2. The method gives a better PSNR value, but it survives for a few attacks only.

In 2017, Xilin Liu et al. [3] implemented a zero watermarking for color images using SVD and Visual cryptography in the DWT domain. In this method, the shares can be generated based on image feature using visual cryptography. The color image is decomposed using DWT and watermark can be inserted in the LL subband. It is more robust against attacks. In the proposed method, the LL subband can divide into 4*4*3 blocks and selected m*m blocks for embedding watermark.

Geum-Dal Park et al. [4] was implemented as a method on lossless codebook based digital image watermarking. The proposed technique is used to solve the ambiguity problem in Xing's methods. Here DWT is used to scramble the host image. The watermark can be inserted in LL subband of the cover image.

Amir Houmansadr et al. [5] and Zinal M. Patel [6] proposed an image watermarking scheme based on the visual cryptography. Here the watermark is split into two shares, according to a visual secret sharing scheme. The share1 is embedded in the host image using the spatial domain. The proposed algorithm is more robust against cropping and white noise attacks.

B. Surekha et al. [7] proposed digital image watermarking for copyright protection of digital images based on the VCs and spatial correlation of color. The watermark can be inserted in the spatial domain by modifying the cover object pixels.

Revised Manuscript Received on February 28, 2020.
* Correspondence Author

B. Jagadeesh*, Associate Professor, ECE Department, Gayatri Vidya Parishad College of Engineering (A), Visakhapatnam, India. Email: bjagadeesh76@gvpce.ac.in

K. L. Sivan Prasad Reddy, ECE Department, Gayatri Vidya Parishad College of Engineering (A), Visakhapatnam, India. Email: shiva.klsp@gmail.com

The secret key inserted by a random selection of pixel in the cover object and the watermark can be inserted in the MSB of the cover image.

Shymalendu Kandar et al. [8] and Rohit et al. [9] according to researchers, the cover image can split to no. of shares and the shares are embedded in enveloping images by modifying the LSB components.

At decryption, all shares are required to reveal the source image. The proposed method is useful for avoiding the unauthorized access of cover images.

In 2016, Alavi Kunhu, et al. [10] In this research paper, a novel image copyright protection algorithm was proposed using visual cryptography and DWT. In this method, the 2D-DWT haar transform is used for decomposing the cover image into RGB layers. The watermark can be split into three shares using visual cryptography. Each watermark shares can be embedded in three layers of a cover image in the wavelet domain

Th. Rupachandra Singh et al. [11] proposed visual cryptography-based watermarking on the DWT domain. Here various parts of a watermark embedding in different regions of a cover image to generate owners share.

Haung Daren et al. [12] This paper discusses the new embedding strategy in watermarking using DWT. Here the low-frequency components of watermark should be embedded in the LL sub-band of the image and remaining should be embedded in higher frequency sub-band.

Karishma Patel et al. [13] according to researchers, a secure key is used during a transaction. The key is generated from the bank agreed host image using visual cryptography. In this, two shares are generated out of which one is stored in the bank database along with customer details. The second share used for the client key. The user can use the key while transaction. Here, the DWT based watermark is used for hiding the owners share securely and extracted when it needed.

DWT domain based dual watermarking algorithm using VC method was proposed by Yanyan Han in 2013 [14]. In this research work, the DWT is used to scramble the blue component of the cover image and two watermarks are inserted in LL and HH bands separately. The second watermark to be split into two shares among them one share can be embedded in LL band and another for copyright. The proposed algorithm is effectively improved in robustness, capacity, and security.

Ajay Kumar Mallick, et al. [15] proposed a watermarking scheme to balance the tradeoff between security and imperceptibility based visual cryptography and SVD. The proposed scheme is the watermark can be split into ‘n’ shares and out of n shares, m shares are embedded in the host image.

In 2007, Ming-shi wang et al. [16] was proposed copyright protection method for digital images. In this research work, the (2, 2) visual cryptography is used to generate the shares for copyright protection of secret data. The SVD can be performed in a center portion of the cover image and gives singular values. The watermark can be inserted in SV of the cover image.

In 2015, Malvika Gupta et al. [17] proposed a method to secure the images based on visual cryptography using DCT. The watermark can be inserted in DCT coefficients.

Sudhanshu Suhas Gonge et al. [18] proposed a method using RSA and AES algorithms with DCT domain. In this, visual cryptography used for encryption of the question paper and the watermark can be inserted in that paper. The proposed method is used for the security of sharing the question papers between the different colleges.

Sunesh, R. Rama Kishor [19] reported a survey on digital watermark based visual cryptography algorithm and mainly focused on (2,2) VCS. The survey discussed various VC techniques; watermark techniques based on visual cryptography.

Jitendra Saturwar et al [20] suggested a method on meaningful No. of shares in digital watermarking. In this, the watermark splits into four encrypted shares based on visual cryptography and each share embed in four different cover images. The watermark can be revealed by overlapping all decrypted share of the watermark.

Yanyan Han et.al [21] proposed a method for color image watermarking based on VCS that generate ownership shares based on pixel separation. The blue component in the host image is separated and applying DCT. The encrypted watermark share can be inserted in DCT coefficients.

A robust image watermarking scheme based on visual cryptography was proposed by Meryem Benyousseff et.al [22]. In this method, the K- level dual-tree complex wavelet transform is used to decompose the cover object and the watermark inserted in a random location of cover objects by modifying the mean values of the LL band. The method is more robust against a different type of malicious attacks.

Ren- Junn Hwang [23] was implemented a method for copyright protection for digital images based on VCS that uses MSB to compare with the mean value of the intensity of the secret image in the generation of master shares.

Ching-Sheng HSU et.al [24] proposed copyright protection scheme for digital images based on the VCs and statistics. The proposed scheme employs a sampling distribution of mean and developed in the spatial domain. The master share can be generated from the cover image using the sampling distribution method and the VCS that uses for generating the ownership share based on the pixel value of the binary secret message from the master share. The proposed method can handle many secret images in one host image.

Rawan I. Zaglou et.al [25] proposed a novel watermark based on visual cryptography. The color image can be converted to HSV and the generated shares can be inserted into the V vector. This method gives better results against filters attack than other attacks.

In 2016, a new and copyright scheme based on the visual cryptography by Azz El Arab El Hossaini et.al [26], steerable pyramid transform is used to decompose the cover image. Here the image is decomposed into 3 scales and 4 orientations. The method is more robust for rotation and filtering attacks better than other methods.

B. Pushpa Devi et.al [27] proposed a robust and blind watermark scheme based on VC for copyright protection of digital images. In this, the secret image can be split into two shares based on the mean value of the pixel. The proposed method is more accurate against for gamma correction and blurring attacks compared to other proposed method.

Vaibhav et.al [28] proposed a method in 2015, the implemented method is image security for multiple data owners. In this, the secret data can be split into ‘n’ no. of shares and all the owners have equal rights for single data.

The shares can be generated using VC. The RSA algorithm is used to generate public and private keys. The proposed algorithm for providing security for the confidential image that has many owners.

Naina Gaharwar [29] was proposed a technique in 2015. In this threshold, the watermark is used. The secret data can be inserted without modifying the cover image content.

Here pixel histogram shifting (PHS) is used to create the gap in host image and watermark can be inserted in the gap. However, it is possible to insert more no. of watermarks on the image. The PHS is used to improve the watermark.

In 2017, B. Pushpa Devi et.al [30] proposed copyright protection of digital image using robust and blind watermarking scheme based on visual cryptography. In this, Arnold algorithm is used for shuffles the pixel location of the binary watermark for better encryption. So, the security of digital images is enhanced. The proposed method gives better results than previous methods.

From the above-mentioned papers, some of the issues are observed in existing models. The issues are

1. Results in loss of resolution while restoration of the secret image.
2. Pixel expansion is one of the major issues in visual cryptography.
3. Portability: the original method is restricted for binary images only, but for color images, the additional process may require.
4. In the case of various attack, the restored shares of the watermark image, it is difficult to detect the original watermark.
5. Embedded the large size of watermark share may cause spoil the image fidelity.

III. IMPORTANCE FOR DATA SECURITY

It is necessary to provide security to digital media. In the present scenario, the advancement in information and communication system various new issues related to security and privacy of data has been raised. The third-party users can access the data and they can easily change the content of original data and it is called as attacks. This makes the data can loss originality of the information. These attacks may be either active or passive. In an active attack, the original data to be modified or false data creation, but in the passive attack, the data can access but not affect system sources. So, it is essential for grant security to digital data while transmitting over the open network, therefore a variety of schemes are introduced to provide security to digital data from the last decades. The digital data can be encrypted at the transmitter and decrypted at the receiver by using different encoding techniques. Generally, watermarking, steganography, cryptography techniques are widely used for encoding. DWT, DCT, SVD are used for embedding.

A. The necessity for Image security

The digital data can be in the form of either image, video or audio and sometimes both. The images are one of the digital data and it is easily accessible by any user and ease of distribution compared to other formats like audio and video, etc. It is necessary to concentrate on providing security for the images in open network to prevent from unauthorized users.

IV. RELATED WORK

A. Visual Cryptography

The visual cryptography is also called as visual secret sharing (VSS). It was developed by Moni Naor and Adi Shamir, who was developed in 1994 [31]. The visual cryptography is another scheme to perform copyright protection. This cryptographic technique is used in the visual sharing of secret visual information such as images, video, printed text, etc. The visual cryptography technique is mostly used in sharing secret images. Here, encrypts process follows different procedures like pixel expansion, separate the pixels, type of secret information, etc. Here a secret image can encrypt into shares and the sufficient shares can overlap to decrypt the secret image. This method involves the image to break into '*n'* no. of shares and n shares are required to decrypt the image by overlaying each of them. Practically, this can be performed by printing each share on separate transparency and then placing all of the transparencies on top of each other to reveal the secret image.

B. Approach and Results

Previously, the visual cryptography performs black and white images only, but to meet today's demand, gray and color images formats also coded. The visual cryptography schemes can be done in (2,2), (n, n) and (k, n). Consider (2, 2) VC scheme, the original image is broken into two random looking shares and two shares are required for decryption of secret data, from these two shares one of the shares can be used as a public key and another one used as a private key. The private key is necessary to reconstruct the original image and who has the private key can get the original image. The public key can be freely distributed throughout the open network. The construction of (2, 2) as given below:

Construction of (2, 2) VCS:

Consider the original image consists of '*m'* no. of pixels. In VC, the white pixel is represented by '0' and the black pixel is represented by '1'. The owner can create two shares S1 and S2 which consists of exactly two pixels for each pixel in the secret image. The shares are generated based on below figure 1. If the pixel is white, the owner can select one row from the first two rows. if, the pixel is black then alternatively chosen one of the rows from last two rows. To overlap, the XOR or OR operation can be used. At (2, 2) VCS, it is difficult to reveal the secret image from any one of the single shares.

Table- I: Partitions for a white and black pixel

Pixel	Probability	Share_1	Share_2	$\text{Share}_1 \otimes \text{Share}_2$
□	50%	■□	■□	■□
	50%	□■	□■	□■
■	50%	■□	□■	■■
	50%	■□	■□	■■

For 2 out of 2 VCs, the basic two matrices can be designed S0 and S1 given below.

$$S^0=\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}$$

$$S^1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

Consider (n, n) VCS scheme, the original image is broken into *n* shares and at decryption, all shares are required. In n out of n VCS, one of the shares can hide to protect the visually shared secret. In this, the hidden share can be used as a key for the "decryption" of the protected image. Consider (k, n) VCS, it is the generalized version of VC. The (k, n) is threshold-based visual cryptography, in this original image encodes into *n* shares such that any *k* or k+1 share enables the visual recovery of the hidden image and it is difficult to reveal the secret image with little or k-1 shares.

Construction of (k, n) VCS:

In (k, n) VC scheme, consist n*m Boolean matrices C0 and C1

$$C_0=\left\{\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}.\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}\right\} \text{ and } C_1=\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right\}$$

From the above two matrices, one of the matrixes is selected based on pixel and it defines the color of m subpixel in each share of n- transparencies. Here (2, 2) VCS is applied to generating more shares.

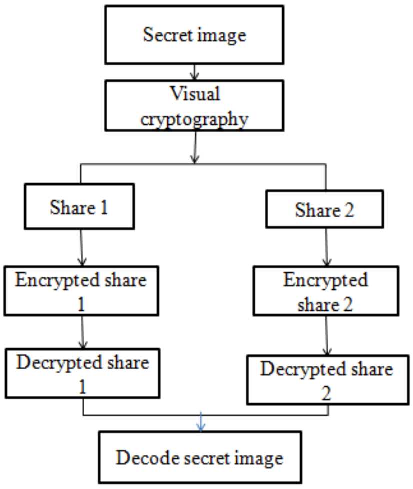

Fig. 1. Methodology for visual cryptography [2]

V. DIGITAL WATERMARKING

Watermarking is a process of hiding the information of the owner in the multimedia to provide proof of ownership. Watermarking is one of the solutions for copyright issues and illegal manipulation of multimedia. In general, the method of embedding and extraction of the watermark can be described as follows. The owner's information can be embedded as a secret watermark into the original data to generate watermarked data. The owner's information can be either secret data, logo, signature or information related to the customer, etc. The owner can keep the watermark and original data concealed and publishes the watermarked data. The following issues arise while embedding and extraction of the watermark.

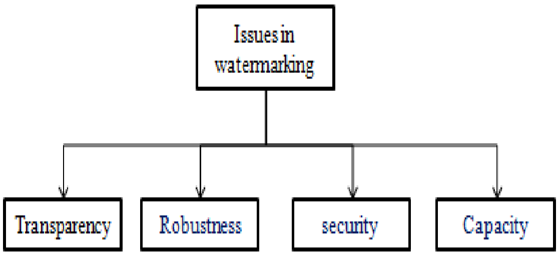

Fig. 2. Issues in watermarking

a. Transparency*:* The transparency is how do we embed watermark and it does not perceptually corrupt the original content?

b. Robustness*:* It describes how data can be embedded and retrieved and how it carries on malicious or accidental attempts at removal.

c. Capacity: How much amount of data that can be embedded in the original data and what is the optimum value of embedding and then extraction?

d. Security: How do we establish the information embedded has not been tampered, forged or even removed by attackers?

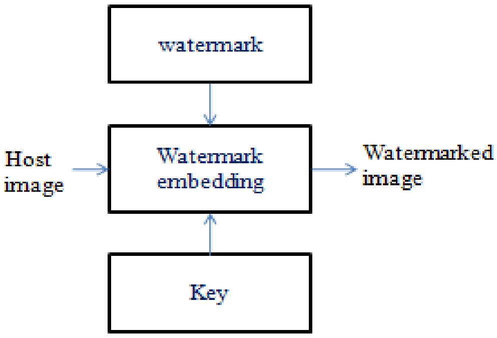

Fig. 3 General block diagram for watermark embedding

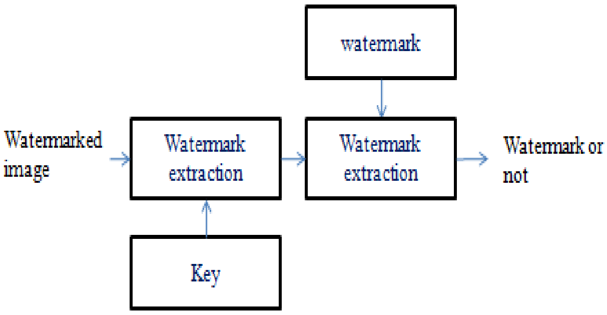

Fig. 4 General block diagram for watermark extraction.

Classification of Watermarking

The watermarks can be classified depending on visibility, type of data to be embedded, the information needed to extract and robustness.

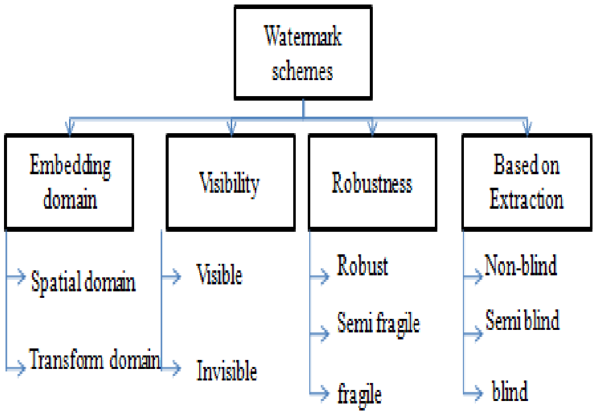

Fig. 4 Classifications of Watermarking schemes [15]

1. Embedding Domain:

Watermark data could be embedded in the spatial domain or in a transformed-domain data

In the spatial domain, the watermark data can embed by changing the pixel value of the cover image. In the transform domain, the transformed coefficients of an original cover image are changed by inserting the watermark and the watermarking techniques contain more robustness against attacks.

2. Visibility:

Depending on the visibility of the watermark data embedded, a watermarking scheme can be classified as a visible or invisible watermarking scheme. In the visible watermarking technique, the embedding of watermark on the original cover image and the watermark can be visual to the human visual system.

In the invisible watermarking technique, the watermark is embedded in the original cover image and it is invisible to the human visual system. In this technique, the original image and watermarked image are mostly looking like the same and the techniques are used for copyright issues than visible watermarks.

3. Robustness:

Depending on its robustness, a watermarking scheme Could also be classified as robust, semi-fragile or fragile. The robust type of watermarks is used for copyright protection and ownership verification because they survive different types of malicious attacks. The Semi-fragile watermarks are more resistant to compression, but reacting quickly to other malicious attacks. The Fragile type watermarks are mostly used for authentication because if any changes in watermarked data, it is not detectable and less robustness.

4. Based on Extraction:

Depending on the extraction of watermark data, could also be classified as for the non-blind watermark technique, the original cover image and private data are required for extraction. However, the cover image is not required, the secret key is enough for the blind watermark technique. The watermark and the secret data are required for the extraction of watermark data in a semi-blind method.

VI. CONCLUSION

In present days, the technology has been increasing day by day. The data can be accessed throughout the world from anywhere. In this, the images are shared over the internet and the malicious users can easily access the sensitive data. The watermarking is the solution to prevent illegal access to digital images, and it is important to combine the visual cryptography techniques for unauthorized access of digital images. In this, the watermark split into the share and embedded in the cover image and after that, it is transmitted throughout the network.

REFERENCES

1. Priyanka Ramesh Shirsat, Mayuri Satish Mundada, Subham Sunil Dipte, G.K. Suryawanshi, “Implementation of DWT-SVD Based Secure Image Watermarking for Copyright Protection Using Visual Cryptography”, in Proc. International Journal for Research in Applied Science & Engineering Technology (IJRASET) -Volume 4 Issue III, March 2016.
2. T. Sowmya, V. M. chandrikanjali, P. Sneha, N. Naveena, Dileep T., “A Combined Watermarking and Visual Cryptography Methods for Copy Right Protection in Digital Images”, SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE), Volume 4, Issue 3, March 2017.
3. Xilin Lui, “Color image zero watermarking based on SVD and visual cryptography in DWT domain”, in proceeding eighth international conference on graphic and image processing, SPIE vol. 225, 2017.
4. Geum-Dal Park, Dae-Soo Kim, Kee-Young Yoo, “Lossless codebook-based digital watermarking scheme with authentication”, in proceeding eleventh international conference on information technology, 2014.
5. Amir Houmansadr, G. Shahrokh, “A Digital Image Watermarking Scheme Based on Visual Cryptography”, an international symposium, 2005.
6. Zinal M. Patel “Image Watermarking Using LSB and Visual Cryptography”, International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2016.
7. B. Surekha, Dr. G. N. Swamy, Dr. K. Srinivasa Rao, A. Ravi Kumar, “A watermarking technique based on visual cryptography”, Journal of information assurance and security 4, 470-473, 2009.
8. Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara, “Visual cryptography scheme for color image using a random number with enveloping by digital watermarking”, international journal of computer science issue. 8, vol. 8, May 2011.
9. Rohit, Dr. K. M. Hari Bhat, Dr. B. K. Sujatha, “Visual cryptography based secured and robust digital image watermarking”, in proceeding international conference on multimedia processing, communication and information technology, 2013.
10. Alavi Kunhu, Nisi k., Sadeena Sabnam, Majida a., Seed Al Mansoori, “Hybrid Visual Cryptography cum Watermarking Algorithm tor Copyright Protection of Images”, Online International Conference on Green Engineering and Technologies (IC-GET), 2016.
11. Th. Rupachnandra Singh, Kh. Manglem Singh, Sudipta Roy, “Image watermarking scheme based on visual cryptography in DWT”, international journal of computer applications, vol. 39 Feb. 2012.
12. Hwang Daren, “A DWT based image watermarking algorithm”, proceeding in IEEE international conference on multimedia, 2001.
13. Karishma Patel, Prof. D. R. Kasat, Dr. Sanjeev Jain, Dr. V. M. Thakare, “Secure transaction using visual cryptography”, international journal of advanced in cloud computing and computer science, vol. 1, issue 2, 2015.
14. Yanyan Han, Wencai He, Qing Luo, “DWT – domain dual watermarking algorithm of color imaged based on visual cryptography”, in proceeding ninth international conference on intelligent information hiding and multimedia signal processing, 2013.
15. Ajay Kumar Mallick, Priyanka, Sushila Maheshkar, “Digital image watermarking scheme based on visual cryptography and SVD”, in proceeding Springer, 2016.

16. Ming-Shi Wang, Wei-Che Chen, "Digital image copyright protection scheme based on visual cryptography and SVD", Optical Engineering, volume 46(6), June 2007.
17. Malvika Gupta, Deepti Chauhan, "A Visual Cryptographic Scheme to Secure Image Shares using Digital Watermarking", in proceeding International Journal of Computer Science and Information Technologies, Vol. 6 (5), 2015.
18. Sudhanshu Suhas Gonge, "Combination of encryption and digital watermarking techniques used for security and copyright protection of still image", in proceeding international conference on recent advance and innovations in engineering, May 2014.
19. Sunesh, R. Rama Kishore, "Digital Watermarking Based on Visual Cryptography: A Survey", in proceeding 5th International Symposium on "Fusion of Science & Technology", New Delhi, India, January 18-22, 2016.
20. Jitendra Saturwar, Dr. D.N. Chaudari, "Deciding a meaningful number of shares in digital watermarking scheme for secret image", in proceeding international conference on signal processing, communication, power and embedding system (SCOPES), 2016.
21. Yanyan Han, Wencai He, Shuai Ji, Qing Luo, "A digital watermarking algorithm of color images based on visual cryptography and discrete cosine transform", in Proc. Ninth international conference on P2P, Parallel, Grid, Cloud and internet computing.
22. Meryem Ben Yousef, Sameera Mabtoul, Mohammed El Marraki, Drissaboutajdine, "Robust image watermarking scheme using visual cryptography in the dual-tree complex wavelet domain" journal of theoretical and applied information technology, vol. 60 Feb 2014.
23. Ren- Junn Hwang, "A digital image copyright protection scheme based on visual cryptography", Journal of science and engineering, vol. 3 pp 97-106, No.2, 2000.
24. Ching-Sheng Hsu, Young-Chang Hou, "Copyright protection scheme for digital images using visual cryptography and sampling method", optical engineering, vol. 44(7), July 2005.
25. Rawan I. Zaghloul, Enas F. Al-Rawashdeh, "HVS image watermarking scheme based on visual cryptography", international journal of computer and information engineering, vol. 2 No. 2, 2008.
26. Azz El. Arab El Hossain, Mohammed El Aroussi, Khadija Janali, Sameer Mbarki, Mohammed Wohbi, "A new robust blind copyright scheme based on visual cryptography and steerable pyramid" international journal of network security, vol. 18 No. 2, Mar. 2016, pp 250-262.
27. B. Pushpa Devi, Kh. Manglem Singh, Sudipta Roy, Y. Jina Chanu, T. Tuithung, "A watermarking scheme for digital images based on visual cryptography", contemporary engineering science, vol. 8, No. 32, 2015, pp 1517- 1528.
28. Vaibhav P. Sapkal, Pooja V. Pundhare, Mahesh V. Samsetwar, Manali A. Teke, Prof. Sonali Patil, "Image security using visual cryptography and watermarking for multiple data owners", International Journal of advanced research in computer science and software engineering, volume5, issue 1, Jan. 2015.
29. Naina Agarwal, Prof. Dr. Reena Gunjan, "Reversible watermarking for digital images using visual cryptography and pixel histogram shifting", international journal of computer science and mobile computing, vol. 4, issue 7, 2015, pp 185-193.
30. B. Pushpa Devi, Kh. Manglem Singh, Sudipta Roy, "New copyright protection scheme for digital images based on visual cryptography" IETE journal of research. 2017
31. Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptography- Euro crypt, PP1-12, 1995.

AUTHORS PROFILE

K. L. Sivan Prasad Reddy, born in 1995, received B. Tech in Electronics and Communication Engineering from the Swarnandhra college of Engineering, Narasapuram, AP in 2016 and received M. Tech in Communication Engineering and Signal Processing at the Gayatri Vidya Parishad College of Engineering (A), Visakhapatnam, AP in 2018. His research interests in digital image processing for data encryption and hiding.

Dr. B. Jagadeesh, received B.E. degree in E. C. E. from G. I. T. A. M., M. E. degree from A. U. College of Engineering, Visakhapatnam, and Ph.D. from JNTUA, Ananthapuramu. He has 18 years of teaching experience and is Associate Professor of ECE Department, Gayatri Vidya Parishad College of Engineering (A), Visakhapatnam, AP, India. He has published more than 30 research papers in various international/national journals and conferences. His research interests include Image Watermarking, Image Compression, and Video Processing.