International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Visual cryptography based on dual image watermarking for copyright protection and security using various transforms

B. Jagadeesh, K. Leela Sivan Prasad Reddy

Abstract*: In this paper, a novel dual image watermarking method is proposed to provide the copyright protection to digital images. In this proposed method, the lower and higher frequency subbands of the decomposed original image are modified by inserting the watermark information using different transforms. The implementation of a method that combines the visual cryptography with dual image watermarking to provide the security for the digital images during an exchange in open networks. The Arnold transform is used to encrypt the second watermark to employ the secure communication. Based on the proposed, the perceptibility and robustness of the distributed images can be increased. The original and watermarked images look like same and the PSNR and NCC are calculated for analyzing the system performance. This method is more robust and secure than existing methods.

Keywords*: Visual Cryptography, Dual Image Watermarking, Arnold Cat-map, Copyright Protection.

I. INTRODUCTION

In the present days, the uses of the internet increased in every field. Due to the less time utilization, the digital data are shared between the devices using public networks. The digital information like audio, images, and videos are comfortable to duplicate and modify. The security issue may arise during the distribution. The security issues like the malicious users can access the data and modify the content of the original data. This is the motivation for doing research in the image processing field and data hiding. The watermarking techniques are used in real time application for data security, secret data communication, copyrights, copy prevention etc.

The digital watermarking is one of the techniques that has been introduced to protect the intellectual property of the digital form. The watermarking has two main processes, embedding and extraction processes.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

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

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

In the watermarking method, the secret information is inserted in the original data, then freely distributed over the open networks.

Here the data is inserted with a secret key based on the owner data and the process is known as embedding process.

The secret data can be either visible or invisible in original data. In the visible watermarking techniques, the watermarks are directly visible to the human visual system and the watermarks can destroy the quality of the host image. These are ease of removal by applying direct image processing attacks. To avoid this problem the invisible watermarking techniques are used. In the invisible watermarking scheme, the owner's information can be hidden secretly in the host data and it can prove copyrights for the data by extracting the secret information.

Based on the watermark insertion, watermarking schemes are generally divided into two main Domains i.e. Spatial domain [1]-[2] and transforms domain. In recent times, the singular value decomposition (SVD) was used in watermarking technique to increase the robustness and transparency. The SVD is the most utilizable numerical analysis method that having a property called the singular values (SVs). The image singular values are difficult to change by performing any simple image processing modification and diminutive agitation is integrated into an image [3].

The Visual cryptography is one of the method, that used for data encryption and is developed in 1995 by Noar and Adi Shamir [4]. In visual cryptography, there are two processes, namely encryption and decryption. At encryption, variety of procedures are performed on the visual information, such as pixel expansion, pixel separation, etc. In the decryption process, it eliminates the complex computation problem. The PSNR is calculated to compare the cover image and watermarked image perceptibility. The normalized cross-correlation is applied to check the robustness of this technique. The visual cryptography based on digital image watermarking [5]-[6] [16] scheme can be used to enhance the security and robustness for the digital images.

In the past years, there were many image encryption schemes using to encryption of images. The Arnold cat's map has been proposed for large size image encryption. In 2004, G. Chen, et al. [7], proposed a method based on Arnold cat map for images. Here, the map extends from 2D Arnold cat's map to 3D map for adjacent round. The algorithm applied "XOR plus mod" operation on each pixel to achieve the diffusion.

The key is schemed by using Chen's chaotic system.

In 2005, Ching-Sheng HSU Young-Chang Hou proposed a method for copyright protection scheme based on VC and statistics for digital images [8] and in 2016, Priyanka Ramesh et al. [9] proposed a method based on visual cryptography using DWT-SVD to provide copyrights for an image.

In 2017, B. Pushpa Devi et al. [10] proposed copyright protection of digital images using robust and blind watermarking that utilizes visual cryptography scheme. In this, the Arnold algorithm is used for shuffles the pixel location of the binary watermark for better encryption. So, the security of digital images is enhanced [11].

The remaining part of the paper consists following section 2. Describes in brief about Preliminaries, 3 Designed Scheme, 4 Experimental Results, 5 Analysis, 6 Conclusion, and References followed in Sec. 7.

II. PRELIMINARIES

The following section gives a brief introduction about the VCs, Digital image watermarking and Arnold Cat Map.

A. Visual Cryptography

In visual cryptography, (2, 2), (k, n) and (n, n) schemes are used for encryption of images based on the requirement. In the (2, 2) visual cryptography scheme, the two shares are generated based on pixel separation, pixel expansion, and type of secret data from the secret image [2], [12], [15], namely public and private shares. In this, one of the two shares is required to reveal the secret data. In (k, n) VCS is the threshold-based scheme. Here, can be split into 'n' no. of shares created from the secret image and 'k' is the threshold. Here 'k' or 'k+1' shares are required to reveal the secret message. In the (n, n) VCS, 'n' shares are generated, and out of 'n' shares, all shares are required to get the secret data [13].

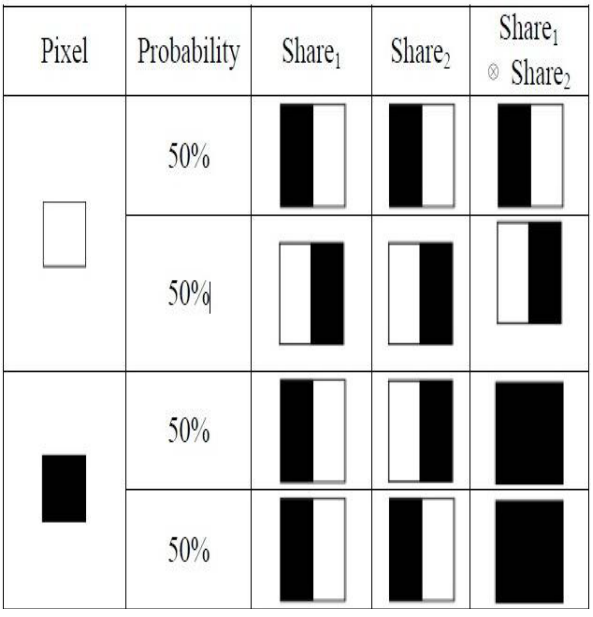


Fig. 1. Partition for Black and White pixels [14]

The VCS schemes are mostly used for authentication, copyright, secret data sharing etc.

B. Digital Watermarking

The digital watermarking is the one of encryption technique for digital data to provide more security. In watermarking, it is difficult to remove the embedded data. The watermarking system has two inputs, cover image and watermark and the watermark can be inserted in two domains, i.e. spatial domain or in transform domain. The watermark data can be embedded in the host image by modifying the image data. In a spatial domain, host image pixels are changed to insert the watermark data and this method can't survive for image processing attacks. To survive from the various image processing attacks, the transform domain is used. In the transform domain, the image can be converted to the frequency coefficients and the watermark pixels are inserted in the coefficients of the cover image. The DWT, DCT, and SVD are mostly used in the frequency domain for embedding the watermark.

C. Arnold Cat Map

The Arnold cat map is the chaotic map that used to change the pixel position without removing the pixels in that image [11]. The main feature on the Arnold cat map is being the image can be randomized to iterations by transformation, but back to its normal after a no. of iterations. The cat map is invertible and the image pixels are shuffled. Compared to Arnold Cat Map, the common encryption techniques are providing less security for the large size of data. Assume that, n*n is the size of the image and the coordinates of pixels are S = {(x, y) | x, y=0, 1, 2... N-1} then Arnold equation is given as,

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N) \quad (1)$$

$$= \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N)$$

Where p and q are the positive integers. If the determinate A is changed, then the (x', y') is the new pixel positions of the original pixel of (x, y).

III. DESIGNED SCHEME

The dual image watermarking technique based on the visual cryptography can be proposed. The design scheme consists of embedding, attacks, and extraction has given below:

A. Watermarking Embedding Technique

Input data: cover object H, watermarks W1, W2

Output data: watermarked data

Step 1: Apply 1-level DWT in the host image. The DWT decomposes the image into four subbands LL, LH, HL, and HH. The LL, HH subbands are selected for inserting the watermarks.

Step 2: Apply the visual cryptography on the watermark1 to generate the two shares. Apply the SVD on HH subband.

$$HH = HU * HS * HV'$$

Apply SVD on share1 of the watermark1 for calculating singular values.

$$WS1 = WU1 * WS1 * WV1'$$

Step 3: Change the SVs of the HH subband of a cover image with embedding strength and apply inverse SVD.

$$HH1 = HS + a.WS$$

Where a is the embedding strength value.

Step 4: Apply the 2D-DCT on LL subband of the cover

image. Modify the DCT coefficients for inserting the watermark2 coefficients.

Step 5: The inverse DWT is applied for combining all the modified subbands to obtain a watermarked image.

The watermarked image can be distributed over the open networks. The design scheme consisting of following blocks shown in Fig. 2.

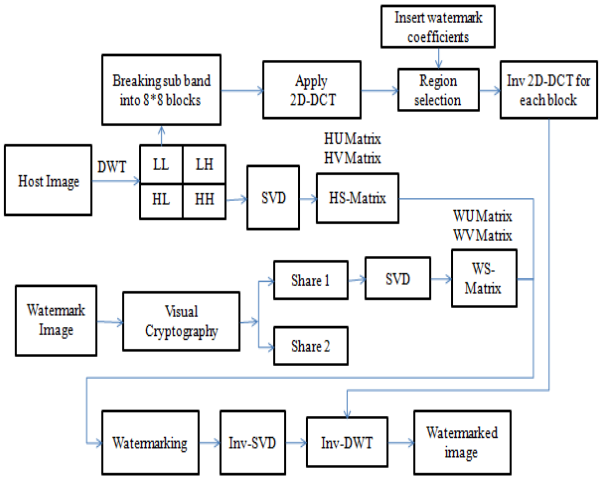


Fig. 2. Proposed Method uses Hybrid Transform

B. Watermarking Extraction Technique

The extraction process is the reverse operation of the embedding technique,

Input data: watermarked image

Output data: extracted watermarks

Step 1: Apply level-1 DWT on the watermarked image, it gives four subbands related to the watermarked image.

Step 2: Apply SVD on the HH sub-band and extract the share1 singular values from HH subband using below Equation. The inverse SVD is performed to obtain the share1 of the watermark1.

$$WS1 = HS - {}^{WS}/_{a}$$

Step 3: Share 2 acts as a private key, is overlapped on the decrypted watermark share 1 to reveal the watermark data.

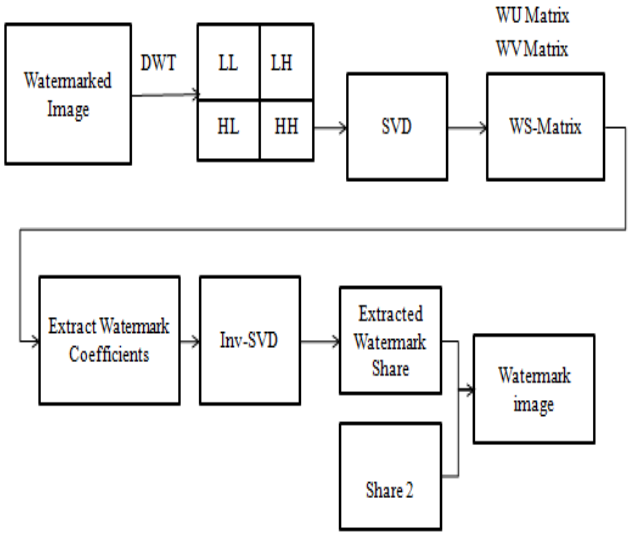


Fig. 3. Extraction of the watermark

IV. EXPERIMENTAL RESULTS

In order to verify the experimental results, MATLAB 2016b is used. Here, seven cover Images and two watermarks are used. In the proposed method, there are two watermarks used for embedded in the cover image. The following images are used as test images and the logos are used as watermark images:

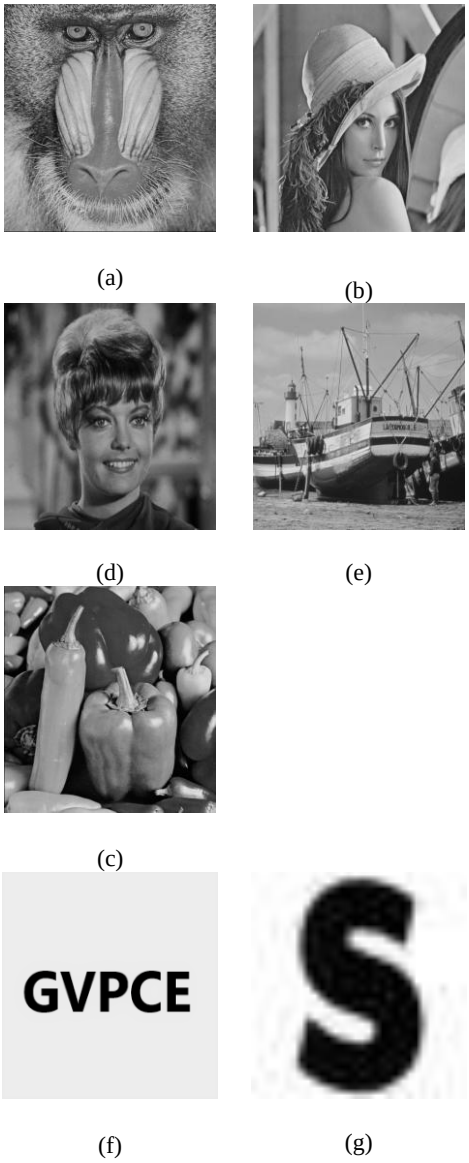
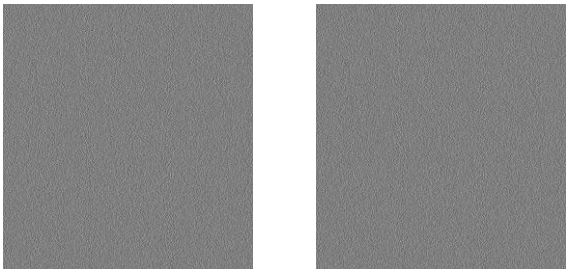


Fig. 4. (a) Mandrill Image (b) Lena Image (c) Peppers Image (d) Zelda Image (e) Boat Image (f) Watermark1 (g) Watermark2

The proposed algorithm utilizes the visual cryptography that enables the original image into two shares. Here the visual cryptography is applied to watermark 1. From out of two shares, one of the share can be embedded in the cover image and another share is used as the secret key.

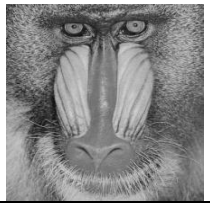
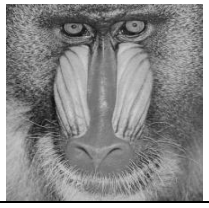


(a) (b)

Fig. 5. Watermar1 Shares a) Share 1 b) Share 2

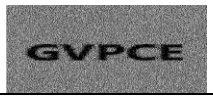
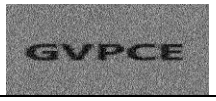
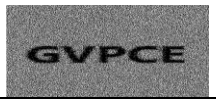
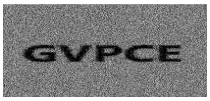
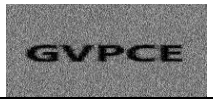
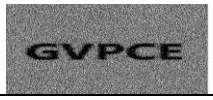
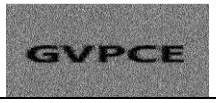
The results are given in Table- I with respective PSNR values for different host images. The PSNR is calculated between the original image and watermarked image. At receiving end, the secret share and extracted shares are overlapped to claim the ownership.

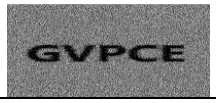
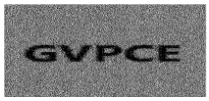
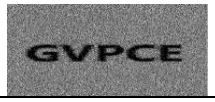
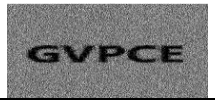
Table- I: The PSNR values of cover images without attacks

S. No	Cover Image	Watermarked Image	PSNR (dB)
1			54.76
2			54.88
3			55.86
4			53.70
5			54.91
6			57.09
7			55.59

The Table- II. gives the different NCC values for with and without attacks. In the proposed method, three noises like Gaussian noise, Salt & Pepper noise, and Poisson noise are added. The method is more robust and it gives better results for all the image processing attacks.

Table- II: NCC values of the watermark with attacks

Type of Attack	Extracted Watermark	NCC
Without Attack		1
Median filtering (Mask Size=1,1/2)		0.9011
Rotation (-75°)		1
Row-column Copying (18,11)		0.9934
Gaussian noise (Variance= 1)		1
Resizing [720 720]		0.9822
Salt & Pepper (Density Value 0.9)		1
Blurring (Mask Size= 1)		0.9461

Gamma Correction (4)		0.99
Row-column Blanking (28, `28)		0.9842
Histogram Equalization		1
Poisson Noise		1

The perceptibility quality of the watermark can be degraded after applying the image processing attacks. The NCC values for different host images are given in Table 3.

Table- III: The NCC values for different host images

Name of the attack	Mandrill	Lena	Pepper
Median Filter	0.90	1	1
Rotation (-75°)	1	0.9046	0.7614
Row column Copying	0.9764	0.9050	0.89
Gaussian Noise (Variance=0.9)	1	1	1
Resizing	0.7918	1	1
Salt & Pepper	1	1	1
Blurring (0.63)	1	0.8854	0.8899
Gamma Correction (4)	0.999	0.9917	0.99
Row-column Blanking	0.9842	0.9395	0.9418
Histogram Equalization	1	1	1
Poisson noise	1	1	1

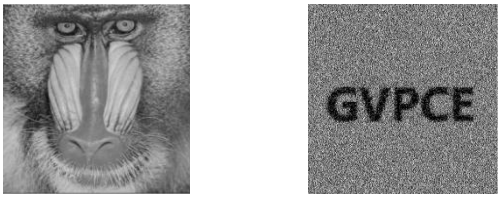
V. RESULTS AND DISCUSSION

Robustness, perceptibility, and capacity are the most important requirements in the watermarking method. The PSNR and NCC are performed to analyze the performance of the method. The proposed watermarking method is checked against different image processing attacks like, row-column blanking, row-column copying, blurring, gamma correction, histogram equalization, salt & pepper noise, Gaussian noise, resizing, rotation, and median filtering attacks and the PSNR and NCC values are calculated.

The PSNR is calculated between the host image and watermarked image to measure the transparency of the images. The proposed method gives better PSNR values for without applying any attacks. The NCC values are calculated to define the similarity between the overlapped shares and the original watermark. The model gives better NCC values against different attacks. The algorithm gives best results for all the above attacks, especially for rotation and any noise addition.

A. Blurring Attack:

In blurring attack, remove the small amount of data from the image. The experimental results for blurring attack are given below:

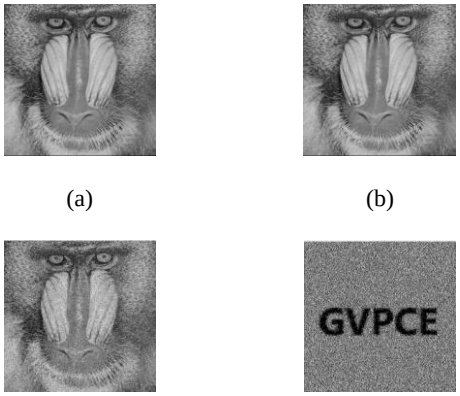


(a) (b)

Fig. 6. Blurring attack. (a) Blurred image (PSNR=16.49) (b) extracted watermark image (NCC= 0. 9461)

B. Noise Addition:

In this attack, three noises i.e. Gaussian noise, salt & pepper noise, and Poisson noise are added to the watermarked image. The method gives better NCC values and poor PSNR values.



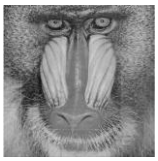
(a) (b)

(c) (d)

Fig. 7. Noise addition to watermarked image. (a) Gaussian noise (b) salt & pepper noise (c) Poisson noise (d) Extracted watermark (NCC=1)

C. Row-Column Copying:

In this attack, the columns are copied as rows as well. The proposed method gives a good NCC value for this attack.




(a) (b)

Fig. 8. Row-Column Copying (a) attacked watermarked image (PSNR=28.88 dB) (b) watermark (NCC=0.9764)

The obtained results are compared with existing systems. In the Table IV, the results are compared with T. Sowmya et .al [13], here the NCC values of the attack Mandrill watermarked image are considered in comparing the results.

Table- IV: The comparison results between the proposed method and T. Sowmya et.al [13]

Name of the Attack	T. Sowmya et.al [13]	Proposed Method
Rotation	0.6754	1
Row-column blanking	0.7047	0.9842
Row-column copying	0.8518	0.9934
Median filtering	0.6427	0.9011

Table- V: The comparison results between proposed method and B. Pushpa Devi et.al [11]

Name of the Attack	B. Pushpa Devi et.al [11]	Proposed method
No Attack	1	1
Filtering Attack	0.996	0.9011
Gamma Correction	0.997	0.9998
JPEG Compression	0.99	0.99
Cropping	0.962	0.98
Rotation	0.986	1
Blurring	0.999	1
Gaussian Noise	0.999	1

Table- VI: NCC values for different host images

Name of the attack	Mandrill	Lena	Peppers
Median filter	0.90	1	1
Rotation	1	0.9046	0.7614
Rowcolumn Copying	0.9764	0.9050	0.89
Gaussian Noise	1	1	1
Resizing	0.7918	1	1
Salt & Pepper Noise	1	1	1
Blurring (0.63)	1	0.8899	0.8854
Gamma Correction (2)	0.99	0.9917	0.99
Row-column Blanking	0.9842	0.9395	0.9418
Histogram Equalization	1	1	1

VI. CONCLUSION

In this paper, a dual image watermarking is proposed based on visual cryptography. The watermarking is proven to be the efficient technique in many applications like copyright protection, secure communication applications, etc. A robust dual image watermarking based on visual cryptography is proposed using the DWT, SVD, and DCT. The Arnold transform is used for key generation and encrypt the second watermark. The proposed algorithm gives good PSNR values for host image and watermarked data based on the NCC values, the model is more robust against different attacks as compared to T. Sowmya et. al [13].

REFERENCES

1. 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.
2. 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.
3. Chin-Chen Chang, Diyu Tsai, Chai-Chen Lin, “SVD- based digital image watermarking scheme”, pattern recognition letters 26, 1577-1586, 2005.
4. Moni Naor and Adi Shamir, “Visual Cryptography”, advances in cryptography- Euro crypt, PP1-12, (1995).
5. 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.
6. Amir Houmansadr, G. Shahrokh, “A Digital Image Watermarking Scheme Based on Visual Cryptography”, 2005.
7. Guanrong Chen, Yaobin Mao, Charles K. Chui, “a symmetric image encryption scheme based on 3D chaotic cat maps”, chaos, solitons and fractals, 749-761, 2004.
8. 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.
9. 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.
10. B. Pushpa Devi, Kh. Manglem Singh, Sudipta Roy, “New copyright protection scheme for digital images based on visual cryptography” IETE journal of research. 2017.
11. Eko Hariyantu, Robbi Rahim, “Arnold’s cat map algorithm in Digital Images encryption”, International Journal of Science and Research (IJSR) 2319-7064, Vol.5, issue 10, Oct. 2016.
12. 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.

13. Ajay Kumar Mallick, Priyanka, Sushila Maheshkar, "Digital image watermarking scheme based on visual cryptography and SVD", in proceeding Springer, 2016.
14. 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", in proceeding SSRG international journal of ECE (SSRG-IJECE) -Volume 4 issue 3-Mar 2017.
15. Simrat Kaur, Rupinder Kaur, "A Review on Trending Cryptography Approaches for Security In Images", in pro. International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 5, Sep-Oct 2017.
16. Abdallah Muneer Elayan, "Robust Watermarking Schemes for Digital Images", December-2013
17. Kulvinder Kaur, Vineeta Khemchandani "Securing Visual Cryptographic Shares using Public Key Encryption", in pro. 3rd IEEE International Advance Computing Conference (IACC) -2013.

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.