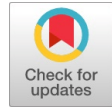


Smart Joint Bank Locker Operation using Visual Cryptography

Sapna B.K, K L Sudha



Abstract: Security has become the foremost vital facet in today's banking system. As a result, banks are committed to give secured banking services to their customers. Considering the case of a joint bank locker operation, it needs a master key owned by the bank to open the vaults along with the key the customers have. To avoid using the manual operation of keys, a visual cryptographic scheme is proposed to operate the vaults using shares. Visual cryptography (VC) hides the details of the image used as a key by generating shares. Image steganography embeds the shares with a cover image, which ensures secure storage of the shares. A completely secured smart joint bank locker operation using a single share owned by the bank is introduced. The shares generated by the bank for different customers are put together to create a unique share to open all the vaults. The proposed approach guarantees not only absolute security than the traditional locker operation but also helps bank a simplified way of maintaining lockers key.

Keywords: PSNR, Shares, Unique share, Visual cryptography.

I. INTRODUCTION

Today, due to rapid growth in the field of banking system a high level of security is an important consideration to the services offered by the bank. One such service is the operation of a safe deposit locker. In the traditional banking system, which is still used in most of the banks in India, to operate a safe deposit box, the bank uses two keys, one kept with the customer and the other with the bank. However, there is a chance that the customer's /officer's key is stolen or lost or misused. If the customer hires the locker jointly then a subset of participants are present for that customer. In that case also the customer is given just one key. There is a chance that one participant might betray the other participant and misuse the locker facility.

With the development of image processing technology and robotics, many smart locker systems have become operational. Most of these smart lockers use biometric features such as fingerprint, face recognition or iris recognition for opening the door to the vault room [1], [2]. This limits the operation to a single person. When a locker is to be opened by the acceptance of multiple authorities such as a company owned by more than one person, the bank has to make some arrangement wherein the lock can be opened

when all of them put their individual keys. Secret key sharing system with visual cryptography (VC) is proposed in papers [3]-[6]. A Collaborative VC scheme where two traditional schemes are merged or glued together is proposed [3] for binary images. A Boolean-based multi-secret sharing (MSS) scheme that encodes n secret images into a universal share and n meaningless shares, and reconstructs lossless secret image is proposed [4] for gray scale images. A multiple secret sharing of color images with no pixel expansion uses watermarking for the authenticity of secret images is discussed in [5]. VC for banking applications is discussed in papers [6],[7] where E-payment system using visual and quantum cryptography is introduced [6]. By generating shares using VC, details of customers are concealed and secure transmission of the password is done by quantum cryptography. Embedded VC system for safe transmission of bank cheque is considered [7] for the binary images. Part II of the paper explains visual cryptography and steganography concepts for the generation of shares. Part III gives details about the proposed system. Part IV provides the method for generation of unique share. Part V deals with results and discussions.

II. VISUAL CRYPTOGRAPHY

VC affords the confidentiality and security for the images used to prevent domination or leakage of confidential information by a single secret-carrier [8]. VC technique encodes a secret image into shares and then distributes them to a number of participants. Each participant gets one share for one secret image [9]. The visual sharing of multiple secrets encrypts more than one secret and thus increases encryption capacity when compared to a single secret. If one participant such as a bank, is involved in more than one scheme then maintaining multiple shares becomes inevitable for the bank. Therefore, it is desirable for the bank to collaborate between its customers to generate a unique share.

Steganography is the process of hiding one image in another image in ways that prevent the detection of the hidden image from the human's eye. Steganography requires two images for embedding secret image in another cover image. First one is a cover image that will hide the secret image. The Second one is the secret image. Combination of a cover image and secret image make a stego-image.

III. PROPOSED SYSTEM

In the proposed system, a gray scale image is used as a secret image for a joint locker operation. A smart locker technique based on visual cryptography is proposed.

Manuscript published on 30 August 2019.

*Correspondence Author(s)

Sapna B.K, Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru, India.

K.L Sudha, Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Smart Joint Bank Locker Operation using Visual Cryptography

All the parties involved with the locker gets a key in the form of an image known as a share. Shares are generated by decomposing the secret image by VC technique. Among these shares, one share is retained by the bank and others are distributed to the participants. The shares distributed to the participants are embedded in cover images to avoid hacking of the shares. If the customer with a subset of participants for one locker form scheme1 then several customers form scheme 2,3N. Each scheme gives one share to the bank. Combining all shares that are retained by the bank, a single unique share is generated. This unique share is used to open all the vaults. When bank share and the shares of all the participants of a single locker are combined, required secret image to open the vault will materialize. A company with three partners want to have a joint locker in a bank. Bank asks the company to give a secret image. The bank generates four shares for the secret image using VC technique. One share is kept in the database of the bank and three shares are distributed to the participants involved in the joint locker scheme. As each participant has one share, the vault can be opened only when the bank receives all the three shares. This requires the approval of all the participants, which increases the security of the operation. Finally, the bank uses four shares to open the vault. As more companies/customers start using the locker systems, the database of shares in bank increases. Instead of using separate share for every scheme, the bank creates a unique share to open all the vaults. This unique share, when combined with their respective shares opens all the vaults. Fig. 1 illustrates the entire system for two schemes using two secret images. Customer1 and Customer2 consists of three participants that allows the bank to create four shares. Unique share is generated by the bank using share S4 of first customer's secret image and share P4 of second customer's secret image. This unique share can be used to open the vault of customer1 as well as of customer 2.

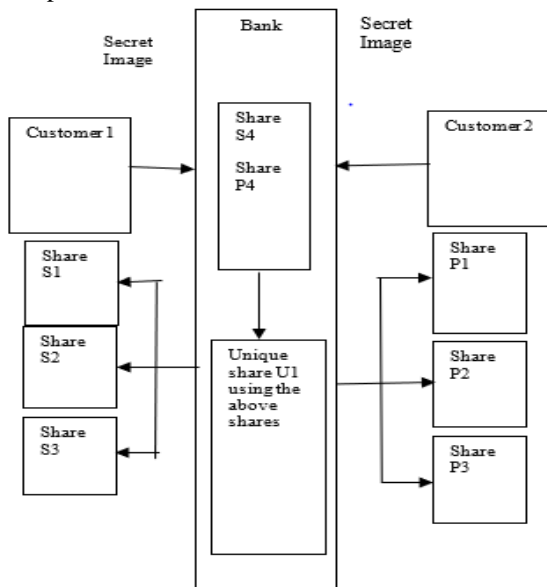


Fig. 1: Proposed system

The steps involved in the proposed method shown in Fig. 2 involves four identities: customer1, bank, database, and locker. Initially, the customer 1 consisting say of three participants wants to use the joint locker system. He sends the secret image to the bank. The bank generates four shares from

this image and distributes three shares S1, S2, S3 to the participants and the fourth one S4 is kept in the bank database. When the customer1 wants to open the locker all three participants must use their shares along with the share stored in the database.

A. Boolean based Visual cryptography for the Share creation process

VC technique uses the Boolean operation to generate shares[10],[11]. The pixel values of the secret image (I) and random matrix (K) are used to generate the resultant matrix (R). The random matrix increases the security of the shares. Two matrices R1 and R2 are created from the resultant matrix. The same process repeated on R1 and R2 creates four shares R3, R4, R5, and R6.

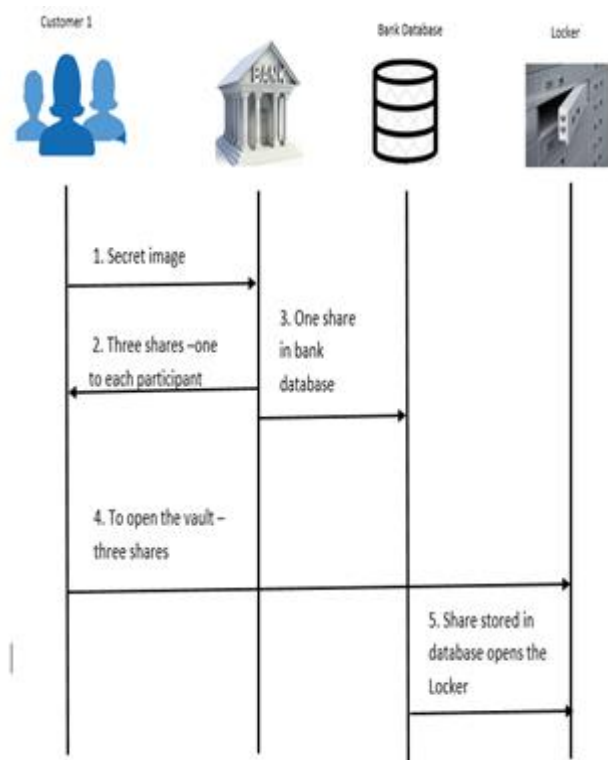


Fig. 2. Steps involved in the proposed scheme

The resultant matrix equation is given by (1)

$$R[i,j] = \text{floor} \left[\frac{\text{floor} \left(\frac{R3(i,j)}{2} \right) + \text{Ceil} \left(\frac{R4(i,j)}{2} \right)}{2} \right] + \text{ceil} \left[\frac{\text{floor} \left(\frac{R5(i,j)}{2} \right) + \text{Ceil} \left(\frac{R6(i,j)}{2} \right)}{2} \right] \quad (1)$$

Since the intensity values of the four matrices are highly correlated share S1 share S2 and share S3 are created by further manipulation of matrices R4, R5 and R6. Unique share is created by R3 that is deposited in the bank database called as S4. To make the shares meaningless they are converted to binary form. But the shares become vulnerable to attacks so they are further protected by nibble insertion steganography technique which achieves additional security.

The three shares S1, S2 and S3 are embedded in three cover images of the participants choice and given to the participants as shown in Fig.3.

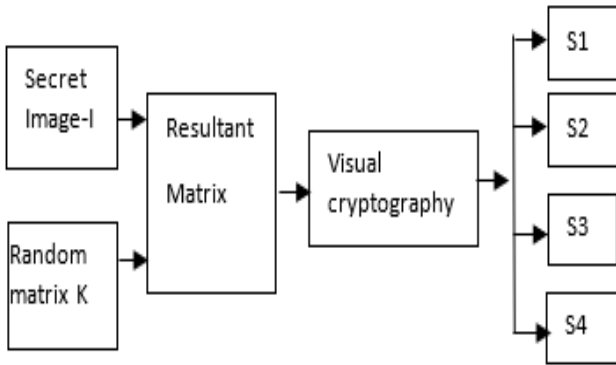


Fig.3. Share creation process

B. Secret Image Recovery Process

The recovery of the secret image involves the extraction of the binary shares from the cover images. Converting these binary values into grayscale values and stacking them together as in (2) reveals the original resultant matrix

$$RE(i, j) = \{[RE3(i, j)+RE4(i, j)+RE4(i, j)+RE5(i, j)]\} \quad (2)$$

Table I. Database contents

Database		U1
S4	SP1	
P4	ST1	
T4	SN1	
N4	•	
•	•	

The random matrix and the resultant matrix uncovers the original secret image by using (3)

$$I = [(K) \oplus (RE(i,j))] \quad (3)$$

IV. GENERATION FO UNIQUE SHARE

Collaboration between the two or more secret sharing schemes generates a unique share, so that common participant holds only one unique share say U1[3],[12],[13]. Two or more secret images of the same size are considered. The Boolean operation based VC scheme generates shares for these secret images.

The bank using VC scheme generates four shares for secret image 1, retains one share S4 with itself, and distributes the other shares S1, S2, and S3 to the individual participants. The same process repeats for the secret image 2. Now the bank has two shares say S4 and P4 from secret image 1 and secret image 2. This can be extended to several images. Fig. 4 shows the process for the creation of a unique share for four secret images. The share of the first customer S4 is stored in the database when the second customer wants to participate his share P4 is also stored in the database. To get the unique share S4 and P4 are XORed. The output is XORed with P4 to

get a unique share. The creation of a unique share for four secret images is achieved by (4)

$$U1 = \{[[[(S4 \oplus P4) \oplus P4] \oplus T4] \oplus T4] \oplus N4] \oplus N4] \oplus \dots\} \quad (4)$$

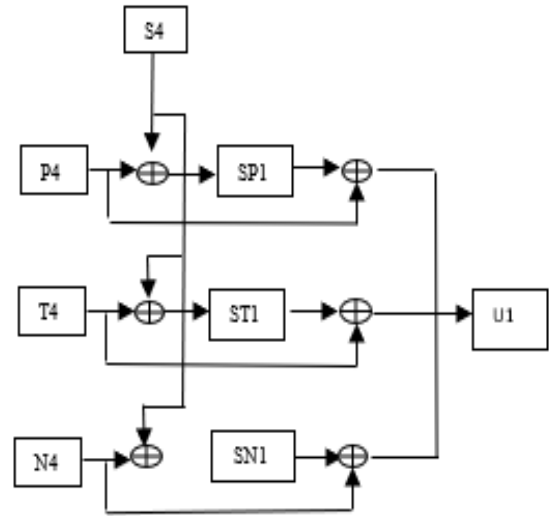


Fig. 4. Unique share creation

The database of the bank stores the step-by-step output is shown in Table. I along with unique share. The intermediate shares SP1, ST1... are also stored in the database. When the customer wants to open the vault the bank retrieves the particular share from the unique share.

For example, to recover secret image 2 the share P4 must be reclaimed. The unique share must be XOR-ed with intermediate share SP1 to recover P4. SP1 must be extracted from the database as in Fig.5.

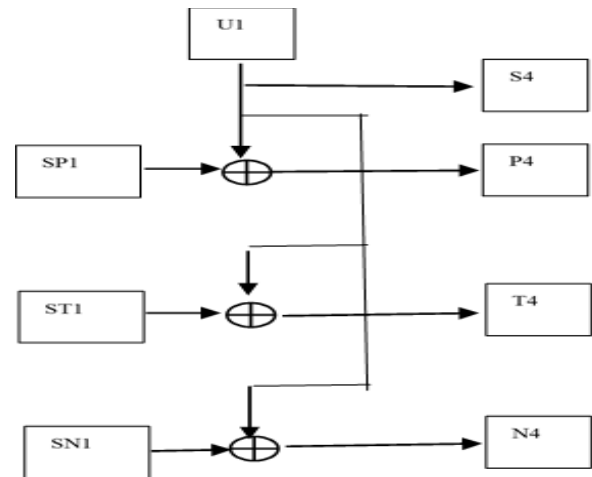


Fig. 5. Recovery of shares

IV RESULTS AND DISCUSSIONS

A. Experimental Analysis

The experimental results of the proposed scheme are shown in Fig. 6 in which the secret image and the random image are of the same size. The shares S1, S2, S3, S4 are obtained from Boolean-based VC technique.



Smart Joint Bank Locker Operation using Visual Cryptography

These shares are secured by embedding them in four cover images to form meaningful shares. Stacking three shares together (S1+S3+S4) or (S2+S3+S4) or (S1+S2+S3) etc., will not give the secret image. The results of this stacking show that the random image emerges slightly but not the secret image.

Similarly, if two shares (S2+S3) or (S2+S4) or (S1+S3) are stacked together the random image is seen more clearly but the secret image is completely hidden. If and only if all the four shares are stacked together, the secret image is recovered without any loss.

The analysis of the shares generated for different combinations is displayed. The PSNR values for the different combination of the shares for Fig.6 are shown in Table II. The PSNR values show that three shares combined will give an image that looks identical but the PSNR values show they are not

Table II. PSNR for different shares for one secret image

share	share	PSNR in dB
S1+S3+S4	S2+S3+S4	26.37
S2+S3+S4	S1+S2+S3	25.47
S1+S2+S3	S1+S3+S4	32.75
S2+S3	S2+S4	26.65
S2+S4	S1+S3	23.88
S1+S3	S2+S3	27.15
S1+S2+S3+S4	Secret Image1	∞

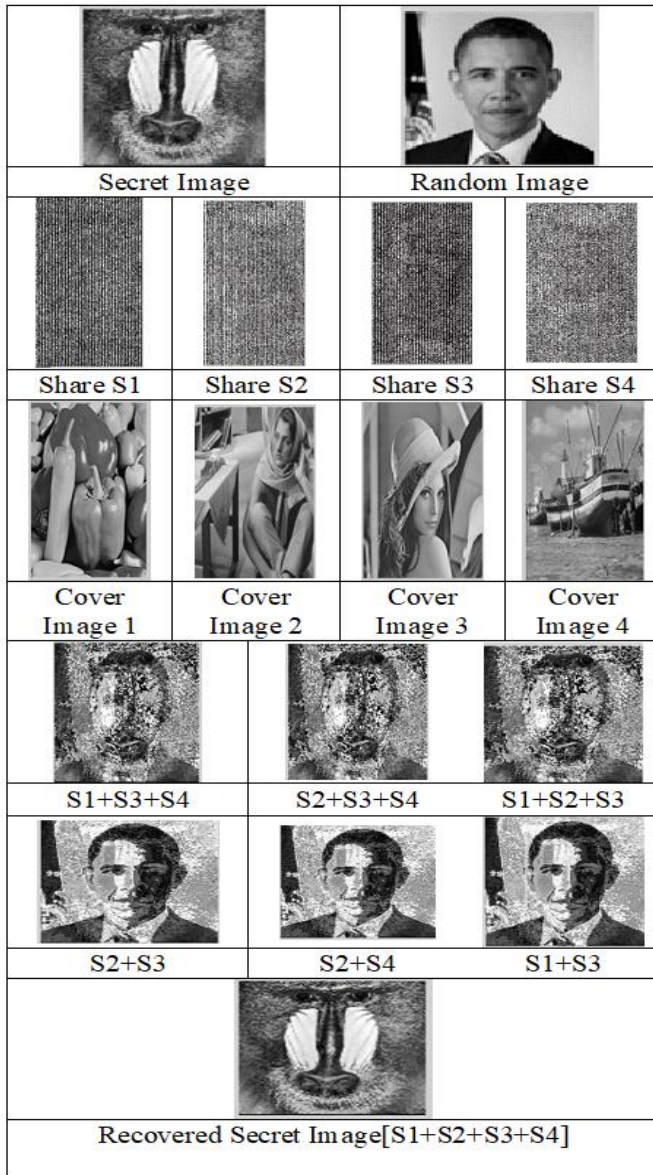


Fig.6. Experimental results for one secret image

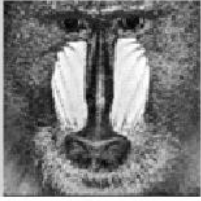



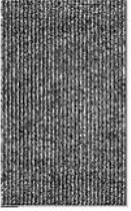


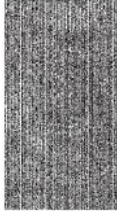


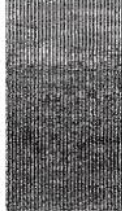

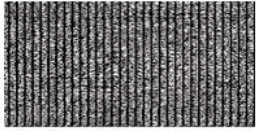






Scheme 1				Scheme 2				
								
Secret Image 1		Random Image		Secret Image 2		Random Image		
								
S1	S2	S3	S4	P1	P2	P3	P4	
								
				Unique share U1				
								
S1+S2+P1+P3		S1+S2+S3+P4		S3+S4+P2+P4		S4+P1+P2+P3		
								
Recovered Secret Image 1 [S1+S2+S3+U1]				Recovered Secret Image 2 [P1+P2+P3+U1]				

Fig. 7. Experimental results for two secret images using unique share

The experimental results of 2 schemes using two different secret images are shown in Fig. 7. The bank provides four shares to each secret image. S1, S2, S3, S4 of secret image 1 and P1, P2, P3, P4 of secret image 2. Unique share is generated by using two shares from each secret image. Fig. 7 also shows that the combination of different shares from both images will not yield the secret image. The unique share with the three shares of the first image (S1+S2+S3+U1) gives back the first secret image. Similarly, the unique share with the three shares of the second image (P1+P2+P3+U1) gives back the second secret image.

For two secret images, the PSNR values for the different combination of the shares are considered in Table III. It shows that the PSNR values decrease when compared to a single image. If two shares from each secret image are considered the value of PSNR is around 9-10 dB which indicates that these shares differ from one another. If three from one secret image and one from the second image is considered the PSNR is about 11-12dB. These results show that even if the hacker gets M-1 shares out of M shares the locker cannot be opened.

Smart Joint Bank Locker Operation using Visual Cryptography

Table III. PSNR for different shares for two secret images

share	share	PSNR
S1+S2+P1+P3	S1+S2+S3+P4	9.93
S1+S2+S3+P4	S3+S4+P2+P4	9.88
S3+S4+P2+P4	S4+P1+P2+P3	11.62
S4+P1+P2+P3	S1+S2+P1+P3	11.58
S1+S2+S3+U1	Secret Image1	∞
P1+P2+P3+U1	Secret Image2	∞

B. Performance Evaluation

The method provides a significant improvement in security compared to the conventional method of using keys. In the proposed method VC method is used to hide the information of the gray scale secret image by converting them into shares which becomes unrecognizable. Use of steganography makes sure that these shares are hidden in cover images, which prevents the hacker from misusing these shares. Consider a hacker gets one share but he cannot use it to open the locker since it requires all the shares of the particular secret image to open the locker. Suppose the hacker gets the secret image even then he cannot guess the method used to generate the shares. It also overcomes the burden of the bank to maintain several shares by generating unique share in collaboration with the customers. Thus the method warrants complete security using visual cryptography, steganography, unique share generation method.

V. CONCLUSION

In this paper, a novel method of using unique share for joint locker operation for banking application is proposed. This system based on visual cryptography and unique share delivers unconditional security by allowing the user to choose a random image along with the input image. Steganography used safeguards the binary shares before distributing it to the participants. The simulation result shows the opening of the locker is solely dependent on the lossless reconstruction of the original secret image. This is substantiated by displaying different combinations of the shares that does not open the locker. The proposed method of smart locker operation can be extended to other banking applications as future work.

REFERENCES

1. D.Binu, M.Arun Athithyan, G.K.Felins, A.Mohammed Anish, D.Sathish Kumar, 2017, "Secure Bank Locker System with Biometrics" IJRST, National Conference on Networks, Intelligence and Computing Systems
2. Raj Gusain, Hemant Jain, Shivendra Pratap, "Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology" 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Date of Conference: 23-24 Feb.
3. Xingxing Jia, Daoshun Wang, Daxin Nie, Chaoyang Zhang, Member, 2016, "Collaborative Visual Cryptography Schemes", 1051-8215 (c), IEEE Transactions on Circuits and Systems for Video Technology

4. Yogesh K. Meghrajani and Himanshu S. Mazumdar, 2016, "Universal Share for Multisecret Image Sharing Scheme Based on Boolean Operation" IEEE Signal Processing Letters, VOL. 23, NO. 10, October 1429
5. Modigari Narendra, Dhanya Ben, C.P. Jetlin, Dr. L. Jani Anbarasi, 2017, "An Efficient Retrieval of Watermarked Multiple Color Images using Secret Sharing", 2017 4th International Conference on Signal Processing, Communications and Networking (ICSCN -2017), March 16 – 18, Chennai, INDIA
6. Shemin P A, Prof. Vipinkumar K S, "E –Payment System using Visual and Quantum Cryptography" International Conference on Emerging Trends in Engineering, Science and Technology, 2016, ICETEST, 2212-0173
7. S.Rajaram, R.Suganya ,2017, " Embedded Visual Cryptography for Secure Transmission of Bank cheque" Proceedings of 2017 IEEE International Conference on Circuits and Systems (ICCS2017), 978-1-5090-6480-9/17, IEEE
8. Ankush V. Dahat , Pallavi V. Chavan, 2015, " Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space" International Conference on Information Security & Privacy (ICISP2015), 11-12 December, Nagpur, INDIA, Procedia Computer Science
9. Xiuqun Wang, Changlu Lin, and Yong Li, 2013," Proactive Secret Sharing without a Trusted Party" 5th International Conference on Intelligent Networking and Collaborative Systems, 978-0-7695-4988-0/13, 2013 IEEE
10. Shankar K, Eswaran P ,2015, "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography" 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS, Procedia Computer Science 70 (2015) 462
11. Jitendra Saturwar, D.N. Chaudhari, 2017, "Secure Visual Secret Sharing Scheme for Color Images Using Visual Cryptography and Digital Watermarking "978-1-5090-3239-6/17, IEEE
12. K. Shankar, P. Eswaran, 2017, "RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography" China Communications , February,119
13. Miss. Nuzhat Ansaria, Prof. Rahila Shaikh, 2016, "A Keyless Approach for RDH in Encrypted Images using Visual Cryptography" International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, India, Procedia Computer Science 78 , 125 – 131

AUTHORS PROFILE



Sapna B.K., presently working as Assistant professor in ECE department, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India. She obtained her Bachelor's degree in Electronics and Communication engineering from Mangalore University and Masters from Visvesvaraya Technological University, and pursuing Ph.D. in Image Processing from Visvesvaraya Technological University, Belgavi, India. Her research interests include image processing, cryptography, security, and wireless communication.



Dr. K. L. Sudha, obtained her Bachelor's degree in Electronics and Communication engineering from Mysore University and Masters from Bangalore University. She got Ph.D for her work on "Detection of FH CDMA signals in time varying channel" from Osmania University, Hyderabad. She has 20 years of teaching experience in Engineering Colleges. She has executed two ISRO funded research projects successfully as principal investigator. She is supervising seven PhD scholars and has guided many post graduate and undergraduate students for their projects. She has published more than 60 research papers in national / International journals and conferences. Her research interests are Wireless communication, coding theory, image processing and chaotic theory.