Development of Visual Cryptography Technique for Authentication using Facial Images

Bhagyashri P. Kandalkar[1], Gopal D. Dalavi[2]

[1](Electronics & Telecommunication Engineering, Amravati, P. R. Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Amravati, India)

[2]Professor, Electronics & Telecommunication Engineering, Amravati, P. R. Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Amravati, India)

Abstract: ***The Cryptography is basically securing the data during the communication between different systems. To provide the security of data during communication in cryptography we together require the Algorithm and Key. Cryptography is the science of maintaining private information whether communicated over secured or unsecured channel from unofficial access, of ensuring data privacy, integrity and authentication, and other tasks. In this project, I am presenting a novel technique of in the Development of Visual Cryptography Using low complexity algorithm(Modular operation), bit shifting algorithm and image is encrypted at Secret sharing method. In encryption secret image is converted into number of share. In this project Secret sharing approach is being proposed for increasing the security of the data. For increasing the security we are basically concentrating on the key part of the cryptography we basically uses the Low complexity and bit shifting algorithm which is designed by the user. Encryption can be perform by dividing number(Total number of pieces of information n=8; The no. of pieces of info which are sufficient for reconstruction k=3) of share . For decryption all the shares are need to be superimposed in proper sequence (for that n=8;k=2).Visual Cryptography (VC) is a technique which encrypts the image and converts it into unreadable format with the help of key by decrypting the image we get original secret image.***

Keywords: Low complexity algorithm, visual cryptography, bit shifting.

1. Introduction

In today fast developing area security play the very important role in the daily life. Everybody know that security of data or information has become a major apprehension nowadays. The security is becoming more important as the volume of data being exchanged. The advancements in universal network environment and in applications the security and privacy of has become progressively more important in today's highly computerized and interconnected world. In present Information Security plays a dynamic role.

Today, more and more digital documents are transmitted and exchanged on internet. It has created an environment that the digital information is easy to distribute, duplicate and modify. Image security becomes a very important issue for image transmission over the internet or wireless network. The security is becoming more important as the volume of data being exchanged. The advancements in universal network environment and in applications the security and privacy of has become progressively more important in today's highly computerized and interconnected world. Information and messages are exchanged over a network. Security has become the important features in communication and other text information these is because of the presence of hackers who wait for a chances to gain an access to private data. Due to the advancements in ubiquitous network environment and rapid developments in cloud computing has promoted the rapid delivery of digital multimedia data to the users. Multimedia data (images, videos, audios, and text.) are of importance for use more and more widely. Now, it is closely related to many aspects of daily life, including education, commerce, defense, entertainment and politics. Hence the security and privacy of Images has become increasingly more important in today's highly computerized and interconnected world.

The most important point in that the computer performed this cryptographic functions, and from this point of view the process become a more secure and more faster. The basic concept of cryptography is the how we can make information unreadable and thus, protected. This will be done by many ways. Some cryptography algorithms are very easy to understand and therefore this algorithm are easily crack. Some cryptography algorithm are highly complex and therefore difficult to crack. One of the best technique for the security of images or text is "Visual Cryptography" .Initially, This technique was developed for black and white images but later on same was extended for color images as well. The (k,n) threshold visual cryptography scheme has been successfully described. Splitting of image into shares is the basic concept of visual cryptography technique. Shares can be meaningful or meaningless depending on the study conducted by different authors. The encrypted image is a noise image so that no one can obtain the secret image without knowing a decryption original image into another form that is difficult to understand. Data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret data, in which the data type of the secret message is an image. But a main issue of hiding data in images is the difficulty to embed a large amount of message data into a single image.

The main objective of this study is to increase security in communication by encrypting the information using a key that is created through using an image. Cryptography presents various methods for taking legible, readable data, and transforming it into unreadable data for the purpose of secure transmission, and then using a key to transform it back into readable data when it reaches its destination [1]. Cryptography is considered to be one of the fundamental building blocks of computer security [2]. The need of reliable and effective security mechanisms to protect information systems is increasing due to the rising magnitude of identity theft in our society. Hence cryptography is a powerful tool to achieve information security, the security of cryptosystems relies on the fact that cryptographic keys are secret and known only to the legitimate user [3]. In secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during encryption and decryption separately, thus, the concept of generating the key from an image came to the role [4]. The main objective of this study is to create a new algorithm to secure connection by using the content of an image. The algorithm uses a color RGB image to generate a key which will be used in the encryption and decryption operations. Our algorithm is distinguished from the other ones as the generated key length varies according to the size of the message and the session type. This makes the encryption algorithm more powerful. The proposed algorithm is simple to implement and easy to use.

In this proposed method Development of visual cryptography technique for authentication using facial images to provide a very high degree of security of image such as hide the image based encryption. In the encryption stage my using secret sharing algorithm. That means it's provide higher security level as compare to hide the image. In that proposed method hacker does not hack data because hide the secure secret image is unbreakable. This provided the more security.

2. Literature Survey

Now a day's many algorithms are obtainable for security purpose using various encryption technique for example simple preservative cipher techniques in to the complicated asymmetric and symmetric key ciphers techniques by using this we increase the security of data or informationVisual cryptography was originally invented and pioneered by Moni Naor and Adi Shamir [5] in 1994 at the Eurocrypt conference. The (k, n) Visual Cryptography Scheme can decode the concealed images without any cryptographic computations. It contain black and white pixel only and it was for sharing single secret. The secret image is divided into exactly two random shares i.e. Share1 and Share2. To reveal the original image, both shares are required to be stacked.

To overcome this problem, G. Ateniese, C. Blundo, A.DeSantis, and D. R. Stinson give a general access structure [6] in 1996. In which given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Until year 1997 visual cryptography schemes were applicable to only black and white images. First gray colored visual cryptography scheme was developed by Verheul and Van Tilborg [7] for sharing single secret.

In 2000 Ching-Nung Yang and Chi-Sung Laih [7], presented new constructions of colored Visual secret sharing schemes. The construction methods are based on the modification and extension of the black & white Visual Secret Sharing schemes and get much better block length than the Verheul-Van Tilborg scheme[6].

Nakajima, M. and Yamaguchi, Y.[],developed Extended visual cryptography scheme (EVS) in 2002. An EVC provide technique to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.

Visual Cryptography Scheme for Grey images by dithering technique was given by Chang-Chou Lin, Wen-Hsiang Tsai[15]in 2003. Instead of using gray sub pixels directly to construct shares, a dithering technique is used .The overall effect of the proposed method is the achievement of visual encryption and decryption functions for gray-level images.

In 2005 Young-Chang Hou and Shu-Fen Tu[16],propose a multi-pixel encoding method for grey-level and chromatic images without pixel expansion. They have utilized two n × r basis matrices to simultaneously encrypt r successive white or black pixels each time.

In 2006 Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo[12],suggested a novel technique named halftone visual cryptography to achieve visual cryptography via halftoning. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing.

In 2007 Shyong Jian Shyua, Yeuan-Kuen Leea,Shih-Yu Huanga Ran-ZanWangb and Kun Chena[13] were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of n>=2 secrets into two circle shares such that none of any single share leaks the secrets.This is the first true result which shows the sharing ability in visual cryptography up to any general number of multiple secrets in two circle shares.

In 2008 Hsien Chu Wu, Hao-Cheng Wang and Rui-Wen Yu [14] proposed a color visual cryptography scheme producing meaningful shares .The scheme uses halftone technique, secret coding table and cover coding table to generate two meaningful shares without increasing the security risks on the secret image.

A new reversible visual secret sharing method proposed in 2009 by Wen-Pinn Fang [15]. It was for sharing multiple secret having black and white image .

Rezvan Dastanian and Hadi Shahriar Shahhoseini 2011[16] proposed Multi Secret Sharing Scheme for encrypting two Secret Images into two Shares.

Anantha Kumar Kondra and Smt. U. V. Ratna Kumari[17] in 2012 Developed an Improved (8, 8) Color Visual Cryptography Scheme Using Floyd Error Diffusion solution which helps to identify the error in the shares and to verify the authentication. however, reorganization of the colorful secret messages having even low contrast.

In 2013 N. Askari, H.M. Heys, and C.R. Moloney[18] proposed An EVC Scheme quality of the share images. The scheme maintains the perfect security of the original extended visual cryptography approach.

In 2014 Shubhra Dixit, Deepak Kumar Jain and Ankita Saxena proposed an approach for secret sharing using randomized VSS in which they propose new visual cryptography algorithm for gray scale image using randomization and pixel reversal approach.

Mr. Praveen Chouksey, Mr.Reetesh.Rai, "Secret Sharing based Visual Cryptography Scheme for color preservation using RGB Color Space", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 5, No5, October 2015.

3. Proposed Methodology

Proposed methodology has been divided into 2 phases.

1. Image Encryption:

In this image encryption phase image is encrypted in three stage. At the first stage we have to select an secret input image, and separate this image into three plan (R plane ,G plane and B plane). At the first encryption phase we have to apply low complexity algorithm , that is modular addition operation(bit OXring) by apply key, this key is inbuilt in system which is only know to the administration (user). Now at second encryption stage we have to apply bit shifting algorithm, there is so many block in the AES algorithm, but am taking the one of the part of them that is mix column operation. In this algorithm pixel can be shift by one first and after it will shift by three. Or in simply for matrix operation, it will directly multiply by 2 and 8. We can get the modified image and now at the first stage encryption apply secret sharing algorithm. The basic idea of visual cryptography is that image is divided into several part called as share. A secret sharing sachems is secret design to share a piece of information or a secret among a group of people in such a way that only authorized group of people can reconstruct the secret from there share . In the secret sharing algorithm we have to separate each channel into eight share(Total number of pieces of information n=8; The no. of pieces of info which are sufficient for reconstruction k=3). The total number of share forming from RGB channel is R+G+B=8+8+8=24, but we have to combine 24 share into RGB 8 share. At the last phase we get the encrypted eight share

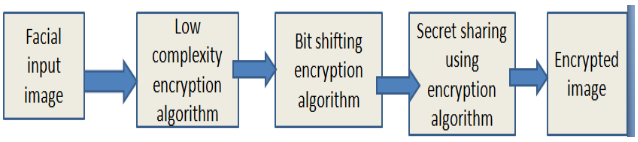

Facial input image
Low complexity encryption algorithm
Bit shifting encryption algorithm
Secret sharing using encryption algorithm
Encrypted image

Figure 1: Architecture for Encryption

2. Image Decryption:

In this decryption stage, I am transmitting this eight encrypted share now we have to apply secret sharing Recovering decryption algorithm. In this algorithm we have to separate eight share into three different channel, each channel can carry 8 share each, mean that we can get the 8 share of R, 8 Share of G and 8 share of B. We can get the total 24 share , now we have to apply each channel inverse bit shifting algorithm, we can get the modified reconstruction image , this is an decryption phase 2. Now at decryption phase 1, We have to apply inverse low complexity algorithm, that is inverse modular operation, in this operation we can do a inverse modular XORING algorithm. The inbuilt key is xoring with the output of encrypted stage, we can get real secret image. At the last decrypted original secret image

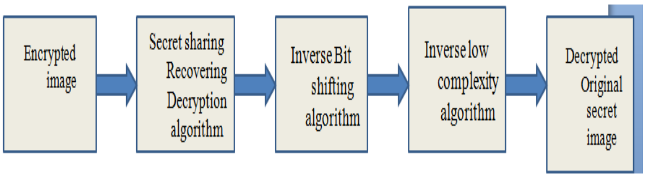

Encrypted image
Secret sharing Recovering Decryption algorithm
Inverse Bit shifting algorithm
Inverse low complexity algorithm
Decrypted Original secret image

Figure 2: Architecture for Decryption

3.1. Block Explanation

3.1.1 Low Complexity Algorithm

In order to enhance the security each encryption round encompasses simple mathematical operation because the designed to be compatible with computing device.At the first encryption phase we have to apply low complexity algorithm, that is modular addition operation(bit OXring) by apply key, this key is inbuilt in system which is only know to the administration (user).

Low complexité algorithm
c=bitxor(A, P)
Where p=constant(key)
Example 1] Bitxoring for encryption
bitxor(13, 100)
ans =105
2]Bitxoring for décryptions
bitxor(100, 105)
ans = 13

3.1.2 Bit Shifting Algorithm:

Now at second encryption stage we have to apply bit shifting algorithm, there is so many block in the AES algorithm, that is The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

But am taking the one of the part of them that is mix column operation. In this algorithm pixel can be shift by one first and after it will shift by three. Or in simply for matrix operation, it will directly multiply by 2 and 8.

Example :1] a=[1 2 3]
a=bitshift(a, 1)
a =[2 4 6]
2]For inverse bit shifting
a=[1 2 3]
a=bitshift(a,-1)
a =[0 1 1]

- The fourth row is shifted 3 bytes to the left in a circular manner.

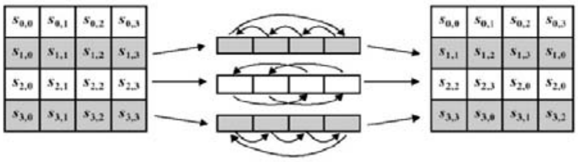

$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,0}$
$s_{2,2}$ $s_{2,3}$ $s_{2,0}$ $s_{2,0}$
$s_{3,3}$ $s_{3,0}$ $s_{3,1}$ $s_{3,2}$

Figure 3: bitshifting by 3

3.1.3 Secret Sharing Algorithm

The basic idea of visual cryptography is that image is divided into several part called as share. A secret sharing sachems is secret design to share a piece of information or a secret among a group of people in such a way that only authorized group of people can reconstruct the secret from there share. Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine the secret might be impractical, and therefore sometimes the *threshold scheme* is used where any of the parts are sufficient to reconstruct the original secret. The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes points to define a polynomial of degree k-1.. Suppose we want to use a (k, n)threshold scheme to share our secret , without loss of generality assumed to be an element in a finite field F of size P where 0 <K<=N<P;S<P and is a P prime number. Choose at random K-1 positive integers a1………..ak-1. With ai<p , and let a0=s Build the polynomial

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_{k-1}x^{k-1}. \text{ L}$$

. Let us construct any points out of it, for instance set i=1…….n ,to retrieve(I,f(i)). Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset of k these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a0.

4. Execution Result

A) Encryption

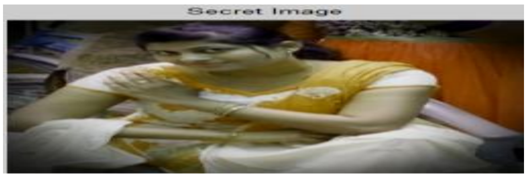


Figure 4: Secret image

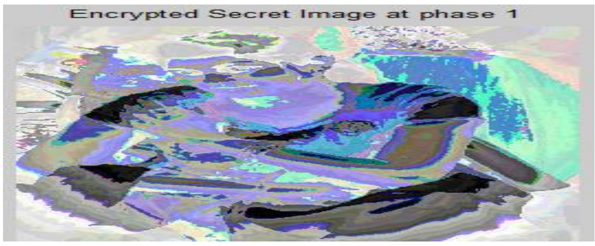


Figure 5: Encrypted secret image at phase 1

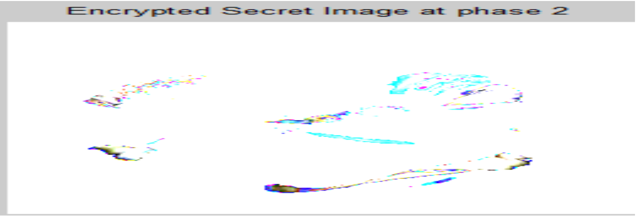


Figure 6: Encrypted secret image at phase 2

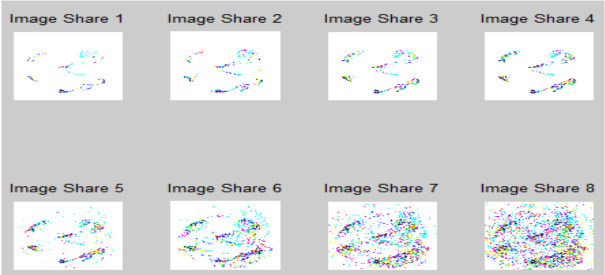


Figure 7: Finally Encrypted image

B) Decryption

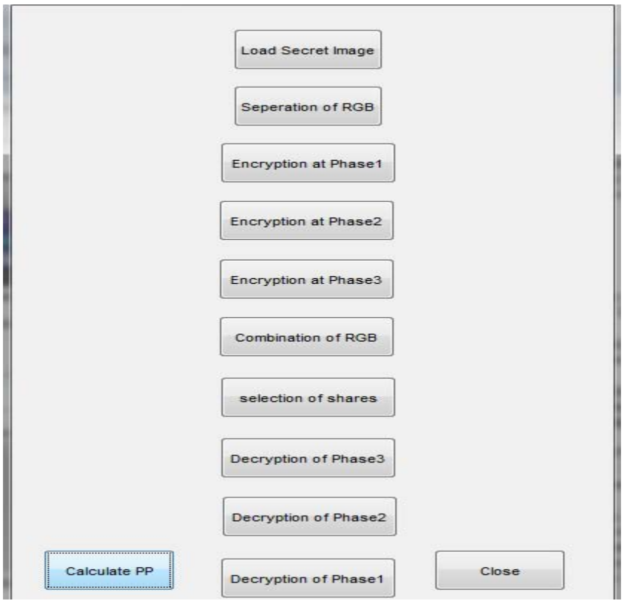
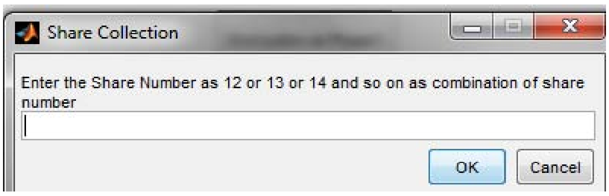


Figure 8: GUI for image decryption



Share Collection

Enter the Share Number as 12 or 13 or 14 and so on as combination of share number

Figure 9: Share selection

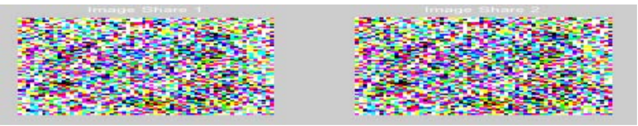


Figure 10: combine share

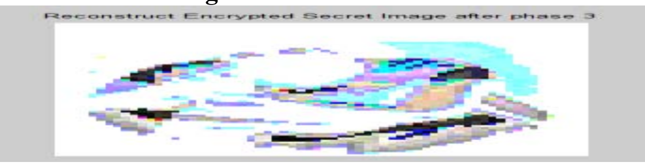


Figure 11: Decryption at phase 3

Figure 12: Decryption at phase 2

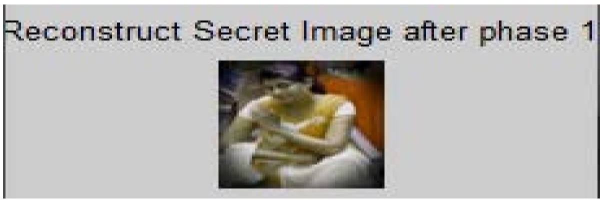


Figure 13: Decryption at phase 1

Elapsed Time Measurement

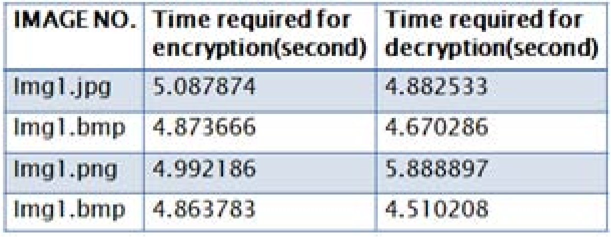


IMAGE NO.	Time required for encryption(second)	Time required for decryption(second)
Img1.jpg	5.087874	4.882533
Img1.bmp	4.873666	4.670286
Img1.png	4.992186	5.888897
Img1.bmp	4.863783	4.510208

5. Conclusion

In today's world where nothing is secure, the security of data is very important. We conclude that all techniques are good for security and have their own advantages and disadvantages and give a security. In this proposed paper we are concentration on Development of visual cryptography technique for authentication using facial images, encryption technique so that it will provide high degree Security for the important messages that can be transmitted over the network securely. This paper adventures the techniques of authentication using Secure facial images. The proposed scheme discovered good security for important messages due to its advance technique and its application use over hear. In this paper we can get the original recover image that is MSE is zero and PSNR is infinite (undefind) .that why we can get more security. In this work new concept of sharing the color image at multiple levels has given which provided more security to the encryption.

6. Acknowledgement

We would like to acknowledge the Faculties of Electronics & Telecommunications Department, P. R. Pote (Patil) Welfare & Education Trust's College of Engineering & Management, Amravati for their support. I Miss.Bhagyashri P Kandalkar. specially want to thank my guide Prof. G.D. Dalvi for their guidance in field of Visual cryptography Engineering and constant encouragement towards the project work.

References

[1] Cryptogrphy and networking security – principal and practices."Willam Stallings" Pearson Education third Edition.

[2] Seshadri,R. and T.Raghu Trivedi "Efficient cryptography key generation using biometric". Int. J. comp.Tech. APPL Vol 2 (1) 183-187.

[3] Asha Ali , Liyamol Aliyar and Nisha V K, "RC5 Encryption Using Key Derived From Fingerprint Image". Computational Intelligence and Computing , 28-29 Dec. 2011.

[4] Santhi, B K.S. Ravichandran , A.P. Arun and L. Chakkrapani," A Novel Cryptographic Key Generation Method Using Image Features", Research Journal of Information Techology 4(2):88-92, 2012.

[5] Mr. Praveen Chouksey, Mr.Reetesh.Rai, *"Secret Sharing based Visual Cryptography Scheme for color preservation using RGB Color Space",* IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 5, No5, October 2015.

[6] Naor, M. and Shamir, A.,"Visual cryptography,"In Proc. Eurocrypt 94, Perugia, Italy, May 912, LNCS 950, pp. 112.,2010, Springer Verlag.

[7] Giuseppe Ateniese ,Carlo Blundo and Alfredo De Santis, Visual Cryptography for General Access Structures, information and computation 129, 86106 (1996), article no. 0076.

[8] E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes," Designs, Codes and Cryptography, 11(2) , pp.179–196, 1997.

[9] C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes," Designs, Codes and cryptography, 20, pp. 325–335, 2000.

[10] Mizuho Nakajima and Yasushi Yamaguchi, "Extended Visual Cryptography For Natural Images," Journal of WSCG. v10 i2. 303-310,2002.

[11] Chang-Chou Lin and Wen-Hsiang Tsai, "Visual cryptography for gray-level images by dithering techniques,"0167-8655/03/$ - see front matter 2003 Elsevier Science B.V.

[12] Young-Chang Hou and Shu-Fen Tu, "A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method," Journal of Research and Practice in Information Technology, Vol. 37, No. 2, May 2005.

[13] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing,Barcelona, Spain, VOL. 15, NO. 8, August 2006.

[14] Shyong Jian Shyu,Shih-Yu Huang, Yeuan-Kuen Lee, Ran-ZanWang, Kun Chen, "Sharing multiple secrets in visual cryptography," doi:10.1016/j.patcog.2007.03.012_ 0031-3203/$30.00 _ 2007.

[15] Hsien-ChuWu,Hao-Cheng Wang, and Rui-Wen Yu,"Color Visual Cryptography Scheme Using Meaningful Shares," Eighth International Conference on Intelligent Systems Design and Applications, 978-0-7695-3382-7/08 $25.00 © 2008 IEEE.

[16] Wen-Pinn Fang, "Non-expansion Visual Secret Sharing in Reversible Style". IJCSNS, VOL.9 No.2, February 2009

[17] Rezvan Dastanian and Hadi Shahriar Shahhoseini," Multi Secret Sharing Scheme for Encrypting Two Secret Images intoTwo Shares," 2011 International Conference

on Information and Electronics Engineering IPCSIT vol.6 (2011) IACSIT Press, Singapore.

[18] Anantha Kumar Kondra, Smt. U. V. Ratna Kumari, "An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion," IJERA ISSN: 2248-9622 Vol. 2, Issue 5, September- October 2012, pp.1090-1096

[19] N. Askari, H.M. Heys, and C.R. Moloney" An Extended Visual Cryptography Scheme Without Pixel Expansion For Halftone Images," 26th Annual IEEE Canadian Conference On Electrical And Computer Engineering Year 2013.

Author Profile

Bhagyashri Pradip Kandalkar Received Bachelor of Engineering in Information Technology from SGB Amravati university & Pursuing Master of Engineering in Electronic and Telecommunication Engineering from P.R.Pote(Patil) College of Engineering & Mgt, Amravati, College of Engineering and Management, Amravati

Prof. Gopal D. Dalvi received the M Tech degree in SSCOE&T College Durg. He now with Prianc in P. R. POTE (PATIL) Welfare & Education Trust's college of polytechnic & Management, Amravati, India.