International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Review Paper on Development of Visual Cryptography Technique for Authentication Using Facial Images

Bhagyashri P. Kandalkar[1], G. 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: ***Cryptography refers to the study of science and art for achieving security by encode the messages to make them the data is not readable. For example the readable message is converted into an unreadable message by using cryptographic system and this process called well-structured and systematic. 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. In this project, I am presenting a novel technique of in the Development of Visual Cryptography Using low complexity algorithm and bit shifting which image is encrypted at multiple levels using low complexity and bit shifting algorithm method. In encryption secret image is converted into monochromatic image i.e. Red, Green and Blue channels are separated and each channel encrypted using low complexity and bit shifting algorithm. It is a bitwise operation. In this project a modified 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. Shares obtain at each level are stored in database using that database image is encrypted to further levels. For decryption all the shares are need to be superimposed in proper sequence using these two algorithms. Sender encrypts the message using the secret key and then sends it to the receiver. The receiver decrypts the message to get the secret information.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. This paper provides a higher level of security for Development of visual cryptography technique for authentication using facial images.***

Keywords: Visual Cryptography, Security, bitwise operation, Cryptography, Encrypting, Decrypting

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.

Images from various sources are frequently utilized and to be transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases are used. These images usually contain private or confidential information so that they should be protected from leakages during the secure transmissions. When an image is transmitted, two common approaches that are applied for secure transmission are image encryption and data hiding. Image encryption is a technique that converts the original image into another form that is difficult to understand. 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 data such as hide the imge based encryption. That means it's provide higher security level as compare to hide the data or information in image form by using steganography. In that proposed method hacker does not hack data because hide the information text in a video form this is unbreakable. As compare to message secure in the form of image and audio in video form gives high degree of 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 information. But hear problem is which technique is well suitable to protect our data for higher level. Visual 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. They use complementary matrices to share a black pixel and identical matrices to share a white pixel. When two shares are superimposed, if two white pixels overlap, the resultant pixel will be white and if a black pixel in one share overlaps with either a white or black pixel in another share, the resultant pixel will be black. This implies that the superimposition of the shares represents the Boolean OR function. In Visual Cryptography Scheme, all n shares have equal importance. It may compromise the security of system.

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. Any k shares from qualified subset of shares can reveal secret information, but less than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can't reveal secret information. The system was more secure and pixel expansion log n.It is also for sharing the single secret having black and white pixel only.

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. Colored secret images can be shared with the concept of arcs or MDS codes. In colorful visual cryptography one pixel is transformed into m sub pixels, and each subpixel is divided into c color regions. In every sub pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacking of sub pixels. For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3.The share generated were meaningless.

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].They improve the pixel expansion from c x 3 to c x 2. This scheme was also developed for sharing a single secret and shares generated were meaningless. 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. It showed a method to improve the image quality of the output by enhancing the image contrast beyond the constraints given by the previous studies. The method enables the contrast enhancement by extending the concept of error and by performing half toning and encryption simultaneously. This paper also describes the method to improve the quality of the output images.

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. Extension of visual cryptography for binary to gray-level ones is useful for wider applications. An input gray-level image is first converted into an approximate binary image by dithering technique, and a visual cryptography method for binary images is then applied to the resulting dither image. This scheme possesses the advantages of inheriting any developed cryptographic technique for binary images and having less increase of image size in ordinary situations. The decoded images can reveal most details of original images. Most visual cryptographic methods utilize the technique of pixel expansion, because of which the size of the shares to be much larger than that of the secret image. This situation is more critical for grey-level and chromatic 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. The probability of these r pixels being colored black depends on the ratio of blacks in the basis matrices. The experimental results show that the shares are not only the same size as the secret image, but also attain the requirement of security. Also the superimposed images have good visual effect.

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.It is Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into n halftone shares carrying significant visual information. The visual quality of obtained halftone shares is observably better than any available visual cryptography method known to date. It maintains good contrast and security and increases quality of the shares.

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. The n secrets can be revealed one by one by stacking the first share and the rotated second shares with different rotation angles. This technique was developed for sharing multiple secret in black and white visual cryptography scheme. 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. The secret image can be decrypted by stacking the two meaningful shares together. This scheme is perfectly applicable and achieves a high security level they extend a single pixel into a 2×4 block. However, the size of the share remains the same as what happens in the 2×2 pixel expansion case. Also a considerable part of the storage space can be saved.

A new reversible visual secret sharing method proposed in 2009 by Wen-Pinn Fang [15]. Without doing any computation, if we stack two transparencies directly, a secret image will appear. Again stack two transparencies but reversing one of transparencies, another secret image will unveil. Different from traditional reversible visual cryptography, the method has advantages and also will not have pixel expansion .They had used Random grid method. Besides, the same idea can be extended to complex style visual cryptography. 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. By stacking two shares, first secret image appears and with stacking one of the shares with 90 degrees rotation in clockwise on other share appears the second secret image. At first, based on halftone technology secret images are transformed secret to binary images then dealer divides secret image1 to two shares, share a and share b, and secret image2 is also divided into two shares, share a', share b'. To make share A, dealer stacks share a' with 90 degrees rotation in counterclockwise on share A and for share B, share b stacking on share b'. Dealer distributes share A and B between two participants and for decryption with present two participants, by stacking share A and B, secret image I appears and stacking share A on share B with 90 degrees rotation in clockwise reveal secret image II.

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. Using CRC algorithm, Color VC scheme and error diffusion method generates the quality shares and diffuses the errors and provides the security from threats like modification, fabrication, interception and shows the good results compared to the previous schemes and increases the security level. Error diffusion is used to construct the shares such that the noise introduced by the preset pixels is diffused away to neighbors when encrypted shares are generated. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share; 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 Without Pixel Expansion For Halftone Images which contain method for processing halftone images that improves the quality of the share images. The size of the share images and the recovered image is the same as for the original halftone secret image. In this scheme the grey scale image is converted to halftone image and simple block replacement and balanced blocked replacement method are applied on it. The scheme maintains the perfect security of the original extended visual cryptography approach. By using an intelligent pre-processing of halftone images based on the characteristics of the original secret image, they have produce good quality images in the shares and the recovered image.

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. (2, 2) randomize visual cryptography in practice where the shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel. The original secret image is divided in such a way that after OR operation of qualified shares we reveals the secret image. In the (3, 3) visual secret sharing scheme shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel and storing the final value of the share pixel after reversal into the shares in round robin fashion. The result of the three shares and after OR operation using stacking of all these qualified shares the original secret reveal.

3. Proposed Methodology

Proposed methodology has been divided into 2 phases.

1. Image Encryption

In this image encryption phase, image is encrypted at multiple levels by using multiple shares. It must be color image i.e. red, green and blue component must be present in that image. The image is converted to unreadable format by splitting secret image into forty shadow images or shares. In general discussion existing work on Development of visual cryptography technique for authentication using facial images in this technique , such as firstly we take a facial image. Then convert it into RGB image. I am applying new method for project , Encryption is carried out by applying key and Low complexity algorithm. After that RGB encrypted image can be segmentated to obtain the RGB channel. It will give the three different channel, this three channel can be encrypted by using three different key and bit shifting algoritham.By this each encryption we get the number of share, to secure the actual image.

At very first step image is converted into monochromatic one by separating all the three channels i.e. Red, Green and Blue. Then we have to encrypts this facial image by using low complexity algorithm. Then each channel is encrypted into eight shares by using key. These eight shares are further encrypted by making group of shares ie. First three shares gives first share, next three shares gives second share and remaining two shares gives third share. In these step total 3 encrypted shares are obtained. Combine three encrypted shares from previous step to get encrypted share of each Red, Green and Blue channel. At last level all encrypted shares from previous step need to combine to produce finally encrypted image. At each stage of encryption the database of previous level shares is required.

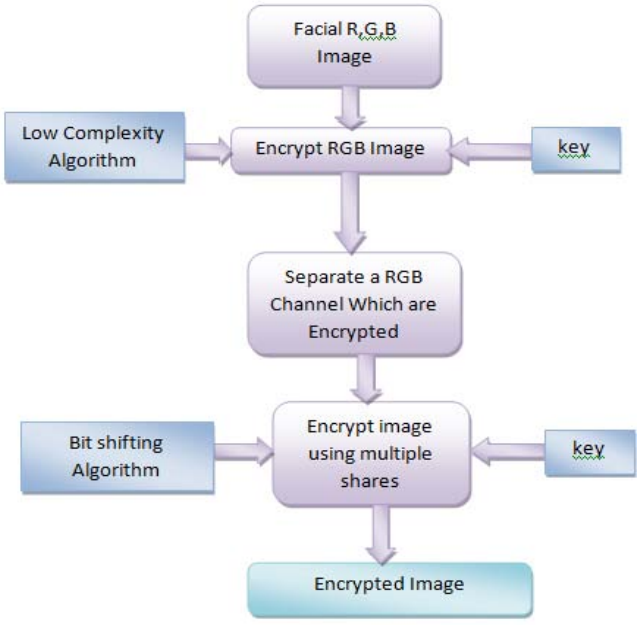

Figure: Architecture for Encryption

2. Image Decryption

The image decryption method work exactly opposite as that of the image encryption phase. Initially encrypted red, green and blue channels are separated from encrypted secret image. Further each channel produces three decrypted shares by using database from previous stage. At this step nine shares are obtained. Each share from previous step decrypted into further shares to give eight shares. The shares get stored in the database for further decryption. The key is used to decrypt eight shares of each color to produce originally separated red, green and blue channel. Combine all the three channels to get decrypted image which is similar to that of secret input image. At every stage of decryption it required database of previous step for performing further operation.

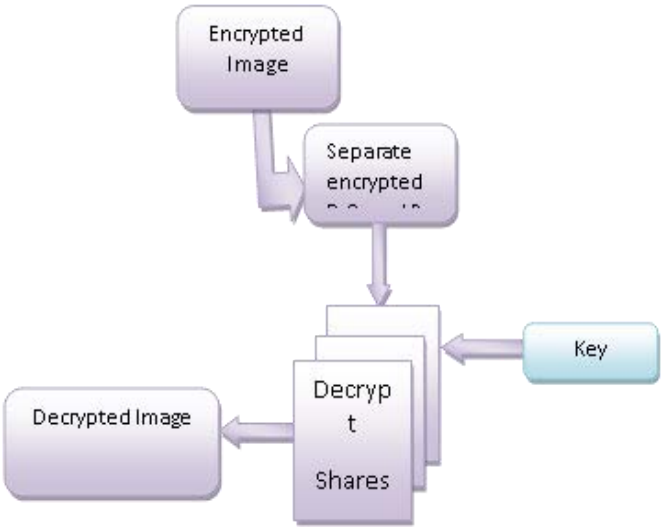

Figure: Architecture for Decryption

4. 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 facial images. The proposed scheme discovered good security for important messages due to its advance technique and its application use over hear. A new algorithm has been suggested that would fulfill all the principles of security and also satisfy the requirements of cryptography .of reconstructed image also pixel expansion and various problems.

In this work new concept of sharing the color image at multiple levels has given which provided more security to the encryption. Encryptions perform by separating Red, Green and Blue channels and then Low Complexity and bit shifting Algorithm is used.

5. Acknowledgement

We thankful to incalculably our management for outspreading their support in providing us substructure and allowing us to use them in the successful completion of our research paper.

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] Naor, M. and Shamir, A.,"Visual cryptography,"In Proc. Eurocrypt 94, Perugia, Italy, May 912, LNCS 950, pp. 112.,2010, Springer Verlag.
[6] Giuseppe Ateniese ,Carlo Blundo and Alfredo De Santis, Visual Cryptography for General Access Structures, information and computation 129, 86106 (1996), article no. 0076.
[7] 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.
[8] C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes," Designs, Codes and cryptography, 20, pp. 325–335, 2000.
[9] Mizuho Nakajima and Yasushi Yamaguchi, "Extended Visual Cryptography For Natural Images," Journal of WSCG. v10 i2. 303-310,2002.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] Wen-Pinn Fang, "Non-expansion Visual Secret Sharing in Reversible Style". IJCSNS, VOL.9 No.2, February 2009
[16] 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.
[17] 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
[18] 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.