International Journal of Pure and Applied Mathematics
Volume 118 No. 8 2018, 277-281
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

Encryption and Decryption of Color Images using Visual Cryptography

M.Karolin[1]
Research Scholar
Department of Computer Science
Alagappa University
Karaikudi, India.
karolinmsc@gmail.com

Dr. T. Meyyappan[2]
Professor
Department of Computer Science
Alagappa University
Karaikudi, India.
meyyappant@alagappauniversity.ac.in

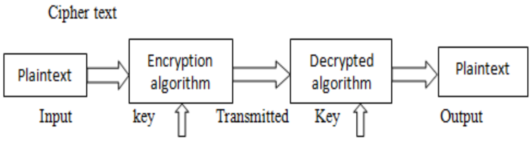
SM.Thamarai
GuestLecturer
Department of Computer Science
Alagappa University
Karaikudi, India.

***Abstract*— The visual cryptography is a type of cryptography that allows digital images to be divided into multiple numbers of printable shares called transparent shares. The images are transmitted after applying the visual cryptographic technique. The hacker cannot understand the distorted image and thus the data communication become secured. It exploits the human visual system to read the secret message from some overlapped shares. This technique overcomes the disadvantage of complex computations required in traditional cryptography. Visual cryptography can also be applied to color images by converting them into black and white binary images. In this research work, visual cryptographic technique is proposed and encryption and decryption are done using Blowfish algorithm. The proposed technique is implemented with Matlab coding.**

Keywords*— *Visual Cryptography, XOR, 16 standard RGB Color Image, Blowfish Algorithm, Encryption, Decryption.

I. Introduction

Visual cryptography is the technique for encrypting user-defined image into multiple numbers of shares called transparent shares. The method was proposed by Naor and Shamir in 1994. It works on the principle that, the user transforms them into printable transparent shares and these shares can be distributed to clients through the communication medium[1]. The most notable feature of this approach that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from few overlapping shares. Thus overcomes the disadvantage of complex computation required in the traditional visual cryptography. The threshold method involved in the visual cryptography makes the application easier and thus reduce the complexity. Visual cryptography for color images basically consist of three phases, namely larger pixel expansion, conversion of the color image to black and white and binary representation of color images. Cryptography includes confidentiality, Integrity, Authentication, Non-Repudiation, Service Reliability and availability[2]. Cryptography methods, processes black and white and grayscale images. The color image encryption and decryption is in the proposed work. Blowfish algorithm is employed for color image encryption and decryption in visual cryptography. The approach of Rijmen preneel indeed can produce visual cryptography for color images. The proposed work uses RGB images.



II. Related Works

Visual secret sharing for color images was introduced by Naor and Shamir based on cover semi groups [10] Rijimen presented a 2 out of 2 visual cryptography scheme by applying the idea of color mixture.

L. N. Pandey and Neeraj Shukla [11], Stacking two transparencies with different colors gives new third color mixture Hou et al. [3] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, They used the binary encoding to represent sub pixels selected for each block and applies the AND/OR operation randomly to compute the binary code for stacking sub pixels of every blocks in the cover image. The code range is from 0to 255 but it can be even larger depending on the expanding factor. Consequently, a secret image can be 256-bit color image.

Sougata Mandal, Sankar Dos and Asoke Nath [4] applied different data hiding algorithm based on visual cryptography. The authors of the paper tried to hide any color message (or) image in two or more shares. Their method is that from one share it impossible to create the second share or to extract the hidden secret message from one share without having the other shares. It may be any for reconstructing password or any kind of important message (or) image.

J. Tamilarasi, V.Vanitha, T.Renuka [5] describe the method for improving image quality in extended visual cryptography for halftone images with no pixel expansion the advantage of their method lies in the term that the same size. It produces less noise in recovering images. By using their method it recovers the images by stacking the grayscale image is taken for the purpose and is converted to its binary representation. To avoid expansion of the images preprocessing has taken place after the halftoning process.

Anantha Kumar, Kondra, U.V Ratna Kumari [6], introduced a new solution that helps to identify the errors in the shares and to verify the authentications. The CRC algorithm and VC scheme with error diffusion method generator the quality of the shares diffuses the error and provides security against the threats like modification of the message, fabrication interception etc. The author developers an encryption method to construct color [EVC] scheme with synchronization. It synchronization the position of the pixels that's Carrey visual color channels of original images across the color channels. So as to retain the original encryption cryptanalysis is also performed to show security concern of the method.

M.karolin, Dr.T.Meyyappan [7], Information hiding in the communication spectrum became a critical task. The Visual Cryptography is a type of cryptography that allows the image to be divided into multiple numbers of shares called transparent shares and then transmission of images. The intruder hence cannot understand the distorted image and thus the data communication becomes secured. The Floyd – Steinberg dithering algorithm is used to manipulate the 256 color code image to reduce it to 16 standard colors code image.

[8] Tingyuan Nie and Teng Zhang, Image encryption and decryption using blowfish algorithm paper is about encryption and decryption of images using a secret-key block cipher called 64-bits. Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times.

[9] I. Ozturk, I.Sogukpinar, Many image content encryption algorithms have been proposed such as DES, 3DES, Blowfish, AES, etc. Blowfish algorithm is highly secured because it has longer key length (more no of key size). The main aim behind the design of this proposal is to get the best security performance tradeoff over existing ciphers.

This template, modified in MS Word 2007 and saved as a "Word 97-2003 Document" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

III. Visual Cryptography Basic Model

In Visual cryptography, a secret binary image is programmed into n shares of arbitrary binary prototypes. It is possible to decode the secret image visually by superimposing a qualified subset of transparencies. Nevertheless no secret data can be acquired from the superposition of an illegal subset [12, 13, 14]. Visual cryptography is a type of cryptography in which image can be securely encrypted by dividing them in a distorted image called transparent shares and transmitted through physically by printing these shares an transparency sheets to the intended user. Visual cryptography assumes in many forms such as for grayscale images, black and white images as well as color images. In the Grayscale model, to ensure the transparencies the white pixels of black-and-white images as transparent. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into a 2x2 black in the two transparencies according to the rules of the basic model. When a pixel is white, the method chooses one of the two combinations of white pixels to form the content of the block in the two transparencies. When a pixel is black, it chooses one of the other two combinations. Then, the characteristics of resulting pixel for two stacked pixels are as follows; black, if both are black white, if both are white black otherwise.

IV. Proposed Methodology

Visual cryptography is a type of cryptography in which images can be securely encrypted by dividing them in a distorted image called transparent shares and transmitted physically by printing these shares on transparency sheets to the intended users. Visual cryptography assumes many forms such as for grayscale images, black and white images as well as color images. The basic model of visual cryptography for color images consists of three phases. The first phase to realize color visual cryptography scheme is to print the color in the secret image on the shares directly. It performs larger pixel expansions which reduce the quality of the divided color image. The second phases converts a color image into black and white image on the three color channels (Red, Green, Blue or equivalently cyan, magenta, yellow) respectively, and then applies the black and white visual cryptography scheme to each of the color channels. This results in decrease of pixel expansion of more number of pixels but reduces the quality of the image due to halftone process. The third phases utilize the binary representation of the color of a pixel and encodes the secret image at the bit-level. This results in better quality but requires devices for decoding process. In the RGB model (Red, Green, and Blue), color images are considered. Floyd Steinberg dithering algorithm is used to transform the 256 code images to low code image. It achieves the dithering using error diffusion and takes the nearest neighbor pixel to create the share. The RGB color code is separated into 16 standard color code formats without reduction in the resolution. The dithering algorithm is used instead of halftoning. Separate array is created to each share and manipulated. This research work extends to the next level to secure the secret image through encryption and decryption using Blowfish algorithm. Matlab tool is employed for implementing the proposed method.

A. *Blowfish*

Bruce Schneier designed blowfish in 1993 as a fast, free different to existing encryption algorithms. Since then it has been analyze considerably, and it is slowly fast acceptance as a strong encryption algorithm. The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no authorize is required. The basic operators of blowfish algorithm include table lookup, addition, and XOR. Blowfish is a cipher based on Feistel rounds, and the plan of the F-function used amounts to a generalization of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64-bit block cipher and is optional as a alternate for DES. Blowfish is a fast and free algorithm and can encrypt data on 32-bit microprocessors. So in this paper, we are implementing blowfish algorithm which is strongest and fastest in data processing store evaluate to other algorithms. Blowfish algorithm is really secured because it has longer key length 32 to 448 bit (more no of key size).

TABLE I. BLOWFISH DETAILS

Algorithm	**Created by**	**Key size**	**Block size**
Blowfish	Bruce Schneier 1993	32 -448	64

B. *Step for share generation processor*

- Consider the input secret image as the RGB model color image.
- The input image is now fed to the error diffusion process that uses Floyd – Steinberg algorithm to diffuse the image.
- Repeat Step-2 until every pixel in the image is decomposed. The dithering process then computes the standard sixteen named color codes.
- According to the traditional method of Naor and Shamir’s black and white VC Schemes, expand each pixel into 2 X 2 blocks arrays.
- This step results in generation of two shares (transparencies) of the secret image.
- Finally, the stacked image is produced by combining the two shares that are generated.

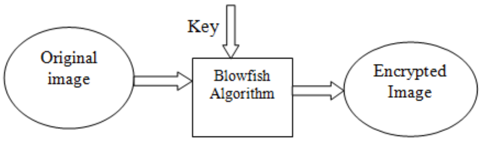
C. *Steps in the algorithm*

- Input the input secret image as the RGB model color image
- Input to the original image.
- Create the key value having 32 to 448 bits.
- Encrypt the image using Blowfish algorithm.
- Decrypt the encrypted image using the same key
- End.

V. ENCRYPTION/DECRYPTION PROCESS

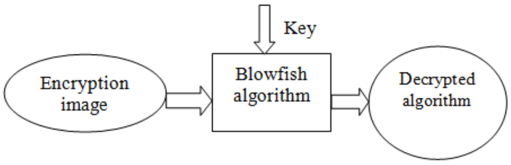
A. *Encryption Process*

Original image and encryption key are input to the encryption process. The bit stream of the original image is separated into blocks length of Blowfish algorithm.



B. *Decryption Process*

The encrypted image is divided into the same block length of blowfish algorithm from top to bottom. The blocks are subjected to decryption function. The same encryption key is used to decrypt the image by reversing the function of sub keys is reversed.



VI. RESULT AND DISCUSSION

The proposed method is experimented with color and monochrome images in JPG, TIFF, Bit Map and PNG formats. Blowfish algorithm is strengthened by increasing the number of rounds. Histograms of encrypted images are found to be dynamic compared to original images. It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte. It can run in less than 5K of memory. The key length is variable, it can be in the range of 32~448 bits: default 128 bits key length. The test result for a sample image is shown below:

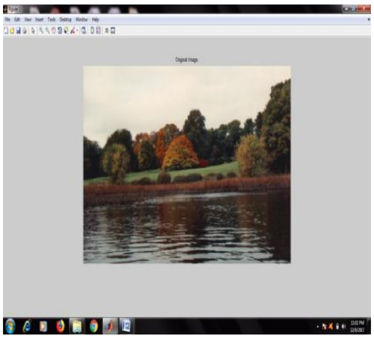


Fig. 1. Original Image

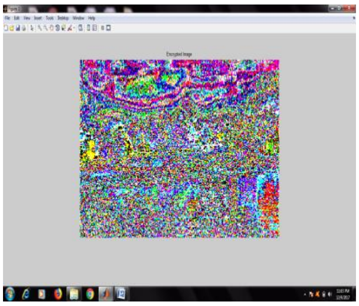


Fig. 2. Encrypted Image

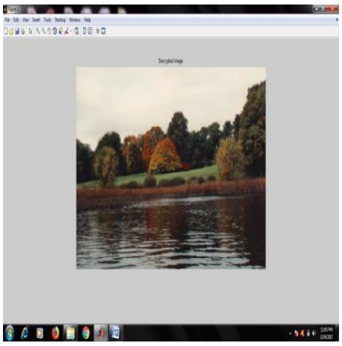


Fig. 3. Decrypted Image

VII. CONCLUSION

In this paper, a visual cryptographic technique is proposed to secure the transmitted digital images. This technique divides the image into multiple printable shares which exploits the human vision system. It overcomes the computational complexity of traditional cryptography. Blowfish algorithm with 64-bit block cipher and key values in the range 32 to 448 is adopted for securing the image. Sample images are subjected to this method. The proposed method is implemented with Matlab coding. Further research is in progress to enhance the process of generating secret shares.

REFERENCES

[1] Shankar, K., and P. Eswaran. “RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography.” China Communications 14.2 (2017): 118-130.

[2] Shankar, K., and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016.Shankar, K., and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016.

[3] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, “Survey of Visual Cryptography Schemes”, International Journal of Security and Its Applications Vol. 4, No. 2, April 2010.

[4] Sougata Mandal, Sankar Das and Asoke Nath, “Data Hiding and Retrieval using Visual Cryptography”, in International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 1, April 2014, pp:102 – 110.

[5] J. Tamilarasi, V. Vanitha, T. Renuka, “Improving Image Quality In Extended Visual Cryptography For Halftone Images With No Pixel Expansion”, in International Journal of Scientific & Technology Research, Volume 3, Issue 4, April 2014, pp:126-131.

[6] Anantha Kumar Kondra, Smt. U. V. Ratna Kumari, “An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion”, in International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012, pp.1090-

1096.

[7] M.karolin Dr.T.Meyyappan,”RGB Based Secret Sharing Scheme in Color visual cryptography”, in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2015.

[8] Tingyuan Nie and Teng Zhang,“ A Study of DES and Blowfish Encryption Algorithm”, IEEE, 2009.

[9] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004.

[10] M. Naor and A. Shamir, “Visual cryptography,” Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, Vol. 950, pp. 1 - 12, 1995.

[11] L. N. Pandey and Neeraj Shukla, “Visual Cryptography Schemes using Compressed Random Shares”, in International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62 – 66.

[12] Shankar, K., and P. Eswaran. “RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique.” Journal of Circuits, Systems and Computers 25.11 (2016): 1650138.

[13] Shankar, K., and P. Eswaran. “Sharing a secret image with encapsulated shares in visual cryptography.” Procedia Computer Science 70 (2015): 462-468.

[14] Shankar, K., and P. Eswaran. “A secure visual secret share (VSS) creation scheme in visual cryptography using elliptic curve cryptography with optimization technique.” Australian Journal of Basic & Applied Science 9.36 (2015): 150-163.