International Journal of Engineering & Technology, 7 (3) (2018) 1696-1699

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.15360
Research paper



A novel approach for securing images using visual cryptographic scheme

Pushpa B. R [1] *, Santhosh Kumar B. J [2]

[1,2]Department of Computer Science, Amrita School of Arts and Sciences, Mysuru Amrita Vishwa Vidyapeetham, India
**Corresponding author E-mail: preeths1@gmail.com*

Abstract

Most applications require exchanging of information over insecure networks. The important issue concerned with respect to the images is to provide confidentiality and integrity. An efficient technique is proposed in order to provide protection to significant images through the digi-tal encryption scheme. Encryption before transmission is necessary for these images such that it makes sure that unauthorized person fails to access to any information. An efficient visual cryptographic approach is proposed for securing images by providing encryption during transferring an images or storing them. The technique proposed ensures that the images are inaccessible by unauthorized persons and also certifies confidentiality. In this proposed method to enhance security during data transmission across the network first the original image gets divided into multiple shares using logic operations and hence encryption technique is employed to these shares to maintain security. The binding of encryption and shares together called as encrypted shares are delivered and at the receiver side the reverse operation is carried out to retrieve back the original image. In the decryption process the decrypted share are layered to extract the actual image and if any shares are lost it is difficult to retrieve the information. The experimental result of the proposed method validates that the method will efficiently encrypt the image with a reduced amount of time without increasing the pixel size.

Keywords: *Encryption; Decryption; Random Key Visual Cryptography; RSA; Images.*

1. Introduction

Most of the organizations are preferring in exchanging digital information over internet that includes transferring of multimedia content such as files, video, audio and images etc .Hence it is significant to secure data over open and unsecured networks to ensure confidentiality of sensitive information. The proposed system can be applied for securing patient's medical information that is considered as sensitive and complex that needs the protection during the data storage, in the cloud and also during transmission across the hospitals. So cryptography techniques can use to provide protection of such data. In cryptography, encryption processes are applied to original data using a procedure to transform data to cipher text that is unreadable form. At the receiver end decryption process are carried out to get back the original data with the help of public or a private key.

There is a huge advancement in the field of Cryptography from the traditional approaches such as Caesar, Trifid and Vigenère ciphers to the current techniques that uses cipher and public key systems such as Diffie-Hellman etc. The cryptography procedure has been adapted to various kinds of digital file formats such as text, images etc. [1].One of the best-known techniques of visual cryptography has been credited to Moni Naor and Adi Shamir.

Visual Cryptography is a cryptographic technique used for encrypting the visual information like picture, text and other multimedia. The basic function of Visual Cryptography is that images are divided into several parts called shares. These shares are distributed among different participants across the media and it is not possible to acquire original information if any unauthorized person tries to access shares and to decrypt. During decryption these shares are stacked together to get the original image back.

2. Literature survey

Quist-AphetsiKester, MIEEE proposed a method for securing medical images. In this method first the input image was operated by a function to generate a secret key. The pixel (RGB) of the original image is shuffled based on the algorithm to which the secret key is applied to produce a cipher text. At the receiver end again a function is applied to decrypt the image. The proposed method was efficient in encryption and decryption process. It is observed that there is a slight pixel expansion in cipher image.

R. Norcen et al introduced a method to encrypt medical images. Here encryption is done in two levels based on AES algorithm. The first part encrypts a subset of bit planes of plain image data and the second it encrypts bit stream of the JPEG image. With this approach of selective bit plane encryption it is observed that up to 50% need to be encrypted whereas in the case of JPEG2000 bitstream encryption the protection of 20% data already provides a sustaining results.

Shankar K et al. here a new approach is proposed to provide great security for the images during transmission. In this approach the RGB value of the secret image is extracted. Each color component R, G and B is represented in the form of matrix by applying some basic operation and a random key matrix is considered. Initially XOR operation of two matrices is carried out to create shares. Then AES algorithm and shares are binded together to get encrypted image and hence security is ensured and also reduces the fraudulent shares of the secret image.

Shital Bet al proposed visual cryptography to provide secured information sharing based on CMY colour based images that breaks down a secret image into several numbers of shares. The original

Copyright © 2018 Pushpa B. R, Santhosh Kumar B. J. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

secret images can be recovered by combining n-1 number of shares out of the n shares the original image can be retrieved. The proposed scheme ensures security as well. The method ensures confidentially that makes it impossible to grab the secret once the shares are generated and distributed across. This results in better performance as compared to RGB colour model.

3. Limitation of the existing system

It is been observed that the existing system proposed works efficiently in securing images using visual cryptographysuch that the shares are more secured and protected from the hacker who can alter to create fake shares but limitation found is that slight change in the ciphered image size and pixel values resulted in a change in the decryption result[1]. And also in the existing system the secrecy of the share is not maintained due to any other fake shares can easily insert or modified. The time required is more for encryption and decryption of shares. Hence our work is carried out in overcoming from these challenges.

4. Proposed method

The proposed scheme provides security of image by incorporating strong encryption and decryption technique. Hence, if someone tries to access any of the shares in unauthorized way it will be difficult to decrypt the information completely without the key and shares. This method imposes security and also the decrypted images are of the same size as original image.

The scheme is divided into three parts:

a) Generation of Shares
b) Encryption of original image
c) Decryption

The proposed method of visual cryptography is employed to send an original image from the sender to the receiver and achieving confidentiality and secrecy of the image. First the RGB color component is extracted from the original image. Each color R, G and B are represented with values (0-255) in the matrix form. Generate key matrix randomly (where m=0 to 255) based on the size of the RGB matrices. Then apply the XOR operation of Key matrix and the input image matrix. The resultant matrices are represented by S1, S2 and S3 to generate the shares. Once all share generation process is done, RSA algorithm is implemented to encrypt the shares and to ensure security for the images and if any shares are missing then it is impossible to get back the original image. These encrypted shares are delivered to the receiving end.

During decryption process, the shares that are encapsulated are extracted by applying the RSA decryption process in order to get three shares and then the reverse operation of encryption is carried out .All these shares are stacked to get the actual image. The proposed method described above is represented in the figure 1.

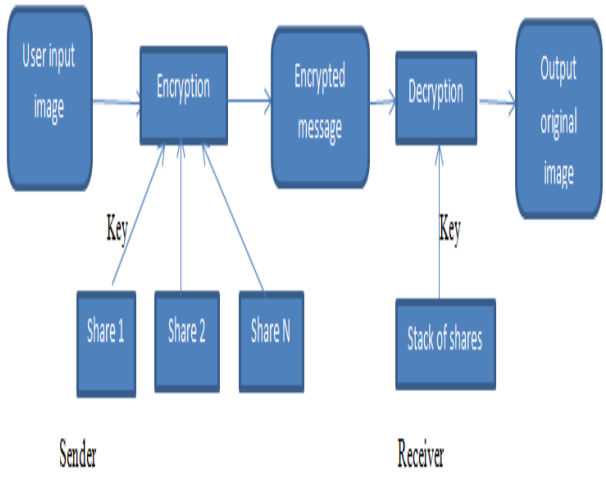


Fig. 1: Block Diagram of Visual Cryptography.

4.1. Generation of shares

Step 1: The R, G and B value is extracted from the original image that can be represented in a matrix form.

B=

113	109	105	102
112	110	107	102
111	112	106	105
115	117	111	106
135	136	135	114

G=

105	101	99	96
103	101	99	95
103	102	97	97
107	107	102	99
129	130	128	108

R=

64	63	58	56
65	65	62	59
63	69	63	62
66	74	68	62
84	89	88	72

Step 2: Generate a random key matrix of the same size as the original image

K=

50	65	45	90
40	45	82	88
72	50	48	70
92	60	95	86
58	85	42	120

Step 3: Applying the XOR operation on Key matrix and R,G and B matrix and store the result in S1, S2 and S3.

S1=

67	44	68	60
88	67	57	62
39	66	90	47
47	73	48	60
189	221	173	10

S2=

30	45	67	79
80	45	50	23
23	30	90	82
58	70	50	12
80	24	11	66

S3=

27	60	12	45
70	54	34	20
80	56	34	20
53	45	60	70
34	15	200	57

Step 4: Shares that are generated in the previous step are subjected to encryption.

4.2. Encryption of original image

RSA algorithm, it is an RSA asymmetric cryptographic algorithm to encrypt and decrypt messages. It provides two different keys for

cryptography. The keys are private and the public key. The public key is shared among everyone across the network, whereas the other key is maintained privately. The public key is used for encrypting the information and to decrypt the message the private key is mandatory.

The procedure for generating a public and private for encryption and decryption is illustrated below with example.

1) Initially the two discrete prime numbers p and q are chosen. The selected integers p and q should be chosen as random number with similar bit length.
2) Calculate n = p ∗ q where n is used as the modulus for both the public and private keys that is expressed in bits.
3) An exponent e should be considered such that e must be an integer and not a factor of n. This creates public key.
4) To generate private key calculate Ø(n) = (p − 1) ∗ (q − 1)
5) Compute d = (k * Ø(n) + 1) /e such that k is an integer
6) Example
7) Let us assume p=7 and q=11 be the two prime numbers.
8) Computing theproduct of two primes p * q = 7 *11 =77
9) Using Euler's totient function compute φ(n)=(p – 1)*(q – 1) = 6 * 10 = 60
10) Choose an integer e such that 1< e < φ (n) where e and n are co-prime.
11) Considering e=7 compute the value of dsuch that (d * e) % φ (n) =1. d= 7 -1 mod 60 = 43
12) The resultant Public key (e,n) = (7,77) and Private key is (d,n) = (43,77)
13) To perform encryption , m = 25 is c = 257 mod 77 = 53
14) For decryption of c = 53 ,m =5343 mod 77 = 25

By applying above procedure the three shares S1, S2 and S3 gets encrypted and hence ensure more security and confidentially in an image. Even if the attacker hacks this shares it is impossible to retrieve the original image.

4.3. Decryption

First RSA decryption is applied, which exactly the reverse order of encryption. The resultant image is the image that was obtained during share generation. The three shares are operating in the following way to get the original image. First share S1 and the key matrix are XORed to obtain B component of the image and then share S2 and key matrix are combined to generate G component and S3 share is XORed with Key matrix to get R component then by combining all these three components R, G and B values into single matrix to extract the original image.

5. Experimental result

The experiment is conducted for the proposed method using c# language. The result obtained is presented in the figure 2. To evaluate the performance of the proposed scheme number of experiments has been carried out with various image sizes types but every time secret color image is retrieved and the time taken to encrypt the shares is less than that of existing system.

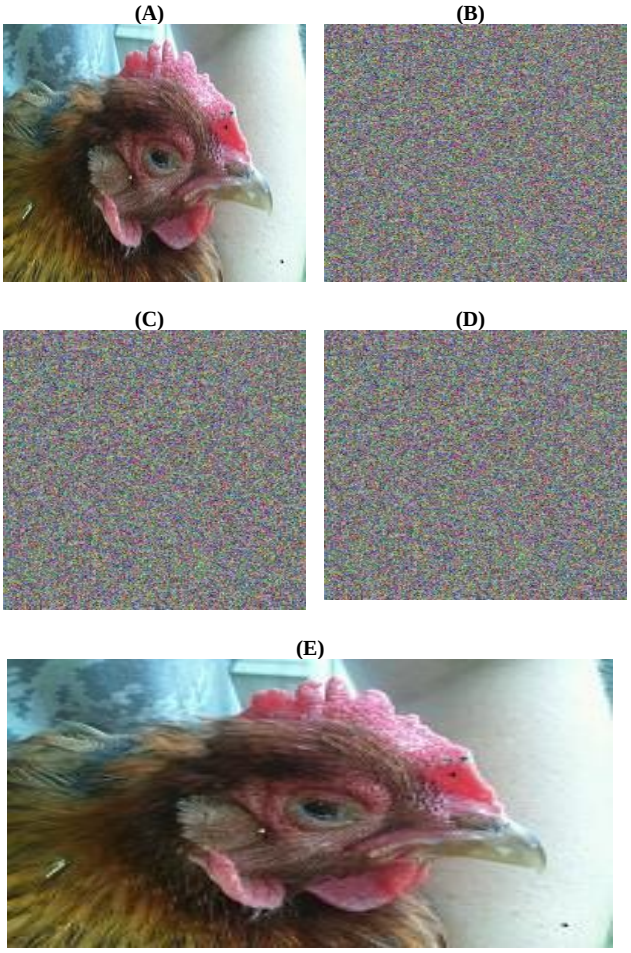


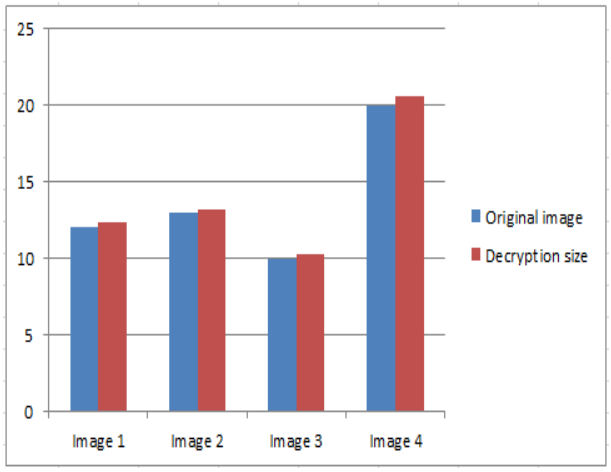
Fig. 2: A) Input Image. B) C) and D) Shares Encrypted Shares. E) Decrypted Original Image.

Comparison of time required for proposed method and the existing system

Method	Security	Shares	Encryption	Decryption
Naor& Shamir (Basic 2×2)	Increase	2	0.82	0.85
Kaur &KhemcHandani's Scheme	Increase	2	0.79	0.80
Proposed	Increase	3	0.86	0.84

From the above table it is clear that the proposed work takes less time for encryption and decryption process.

The graph represents a slight pixel change in original image and the decrypted image.



6. Conclusion

The proposed method coverts the original method to non-readable format. The encryption and decryption process was carried out effectively for the images A novel approach is implemented to generate a shares efficiently. It provides the combination of visual cryptography scheme to generate shares and encryption of shares is carried out to enhance security. There is no much pixel expansion in encrypted image. The shares are created by using random key and hence RSA encryption process is applied to increase the complexity. From the experimental analysis, it is observed that it occupies less memory utilization takes short span of time for computation.

Acknowledgment

The authors are grateful to Amrita Vishwa Vidyapeetham, Mysuru for the support given for doing the research. We are also thankful to our colleague for giving the valuable inputs in our work. We thank our family members and friends for their kind support.

References

[1] Quist-AphetsiKester, MIEEE "A Visual Cryptographic Encryption Technique for Securing Medical Images", in "International Journal of Emerging Technology and Advanced Engineering" Volume 3, Issue 6, June 2013.

[2] R. Norcen et al "Confidential storage and transmission of medical image data" inComputers in Biology and Medicine 33 (2003) 277 – 292. https://doi.org/10.1016/S0010-4825(02)00094-X.

[3] M. Sukumar Reddy et al " Visual Cryptography Scheme for Secret Image Retrieval " in International Journal of Computer Science and Network Security, VOL.14 No.6, June 2014.

[4] Shankar K et al "Sharing a Secret Image with Encapsulated Shares inVisual Cryptography" inInternational Conference on Eco-friendly Computing and Communication Systems, (2015) 462 – 468.

[5] Shital B. Pawar, Prof.N.M.Shahane, "Visual Secret Sharing Using Cryptography" International Journal of Engineering Research (ISSN: 2319-6890) (online), 2347-5013(print) Volume No.3, Issue No.1, pp: 31-33.

[6] Ankush V et al. "Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space" inInternational Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015,

[7] G. Elavarasi, Dr. M. Vanitha, "A Novel Method for Securing Medical Image Using Visual Secret Sharing Scheme", International Journal of Engineering and Technology (IJET).

[8] A. Nandakumar, Harmya, P., Jagadeesh, N., and Anju, S. S., "A secure data hiding scheme based on combined steganography and visual cryptography methods", Communications in Computer and Information Science, vol. 191 CCIS, pp. 498-505, 2011.

[9] A. Shamir, "How to share a secret", Commun. ACM, vol.22 (11) 1979, pp.612 - 613. https://doi.org/10.1145/359168.359176

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

[11] C. Blundo, A. D. Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett, vol. 75, no. 6, pp. 255–259, 2000. https://doi.org/10.1016/S0020-0190(00)00108-3.

[12] SavitaPatil and JyotiRao,"Extended Visual Cryptography for Color Shares using Random Number Generator," International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, pp 399-410 Issue 6, August 2012.