www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12750-12753

Proposed Method for Securing Image Using Visual Cryptography

Ankush Sharma[1], Aarti Devi[2], Anamika Rangra[3], Gandharv Singh[4]

[1]Carrer point University, School of computer science and Engineering,
Bhoaraj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India
ankushasp@gmail.com
[2] Career point University, School of computer science and Engineering,
Bhoaraj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India
aarti_rana88@yahoo.co.in
[3] Career point University, School of computer science and Engineering,
Bhoaraj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India
anamikarangra@hotmail.com
[4] Career point University, School of computer science and Engineering,
Bhoaraj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India
shiny21oct@gmail.com

Abstract: *With the rapid growth of digital media, it is becoming more prevalent to find a method to protect the security of that media like images. An effective method for securely transmitting images is Visual Cryptography. The first algorithm in the field of Visual Cryptography was proposed in 1994 by Naor and Shamir. After this many method has develop in the field of Visual Cryptography Information. In this paper we have proposed new method for securing image. For this we have use Net Beans IDE 7. This method provides good security for image by using simple (2, 2) secret sharing scheme.*

Keywords: quadrants, Visual cryptography, Secret sharing, Share.

.

1. Introduction

Cryptography is a concept to protect data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security. [1][2][3]

1.1 Cryptography

Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control and so forth.[2] In technical terms, the process of encoding plain image message into cipher (encrypted image) messages is called as Encryption. Fig 1.1 illustrates the idea. The reverse process of transforming cipher (encrypted image) message back to original image message is called as Decryption. Fig 1.1 illustrates the idea. [4]

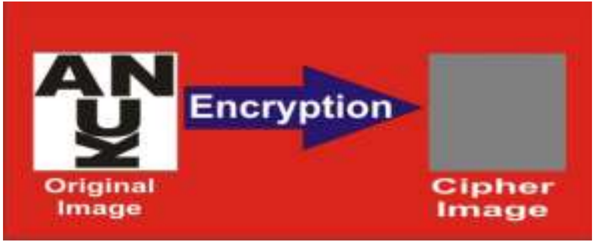

Fig 1.1

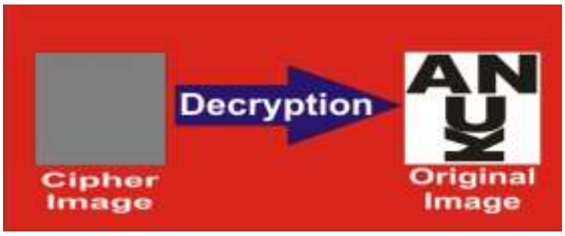

Fig 1.2

1.2 Visual Cryptography

Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers [5]. Human visual system acts as an OR function. If two transparent objects are stacked together, the final stack of objects will be transparent. Changing any of them to non-transparent, the final stack of objects will be non-transparent [6].

1.2.1 EXISTING SHARING SCHEMES

This idea of secret sharing was proposed by Adi Shamir [7] and G. Blakley [8] in middle of 1979. In 1983 another method for secret sharing was proposed by Asmuth and Bloom [9].Shamir‟ scheme is based on Polynomial Interpolation; Blakley scheme is based on hyper plane geometry where as Asmuth-Bloom scheme is based on Chinese Remainder theorem.

(2, 2) secret sharing [3]

This scheme divides the secret information S into 2 shares

Let us suppose that these parts are, S 1, S2 in such a way that Knowledge of any all 2 shares can reveal the secret information.

Knowledge of 1 share will not reveal the secret information.

(2, n) secret sharing [10]

This scheme divides the secret information S into n number of shares

Let us suppose that these parts are, S 1, S2……Sn in such a way that Knowledge of any 2 shares can reveal the secret information.

Knowledge of 1 share will not reveal the secret information.

(k, n) secret sharing[11]

This scheme divides the secret information S into n number of shares

Let us suppose that these parts are, S 1, S2……Sn in such a way that

Knowledge of k or more shares among Si (i n) can reveal the secret information.

Knowledge of less than k shares reveals no information about the secret share.

This technique is called (k, n) secret sharing [10].

(n, n) Secret sharing [12]

This scheme divides the secret information S into n number of shares

Let us suppose that these parts are, S 1, S2……Sn in such a way that Knowledge of n shares can reveal the secret information.

Knowledge of n-1 shares will not reveal the secret information.

2. Proposed Work

Quadrant Based (2, 2) Secret Sharing Visual Cryptography Scheme

In this proposed technique we use (2, 2) secret sharing method for encryption and decryption. In this technique we divide the original Image in to 4 quadrants say Iq1, Iq2, Iq3, and Iq4

Encryption:

This technique has the following steps:-

Step 1: Divide original Image into 4 different quadrants i.e. Iq1, Iq2, Iq3 and Iq4.

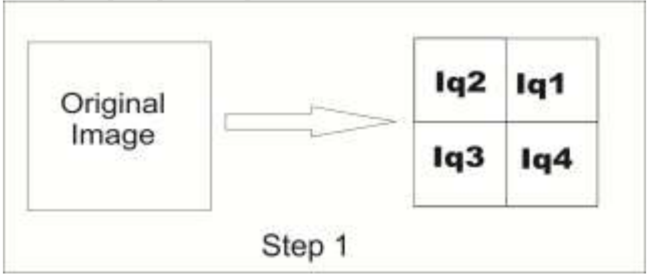

Fig 2.1

Step 2: Take the first quadrant of the original image i.e. Iq1 and encrypt the 1st quadrant with (2, 2) cryptography technique. When we apply (2, 2) secret sharing technique we get share1 and share2 of the 1st quadrant.

Step 3: Take the second quadrant of the original image i.e. Iq2 and encrypt this 2nd quadrant with (2, 2) secret sharing technique. When we apply (2, 2) visual cryptography technique we get share3 and share4 of the 2nd quadrant.

Step 4: Take the third quadrant of the original image i.e. Iq3 and encrypt the 3rd quadrant with (2, 2) cryptography technique. When we apply (2, 2) secret sharing technique we get share5 and share6 of the 3rdquadrant.

Step 5: Take the fourth quadrant of the original image i.e. Iq4 and encrypt the 4th quadrant with (2, 2) cryptography technique. When we apply (2, 2) secret sharing technique we get share7 and share8 of the 4thquadrant.

After applying these steps we get the original image in the encrypted form. If we divide the original image in 4 quadrants then we get the 8 number of shares.

In general we can say that if an image is divided into AN number quadrants then after apply (2, 2) visual cryptography technique we get 2AN number of shares

Mathematically we can say:-

By using "Quadrant Based (2,2) Secret Sharing Visual Cryptography Scheme"

If we divide Original image in AN quadrants.

Number of shares = 2AN.

Decryption:

In this process of decryption we retrieve the original image by stacking the shares of the relevant quarter. After applying encryption we got 8 shares and original image is retrieve only by superimposing the share that are related to that quarter.

We have shares as follow share1, share2, share3, share4, Share5, share6, share 7 and share8.

Step1: We take share 1 and share 2. If we have divide the image in 4 quadrants that means we have 2*4 numbers of shares. And each quadrant must have two shares. So share 1 and share 2 are related to the 1st quadrant. By stacking share 1 and share2 we get the 1st quadrant of the original image.

Step2: We superimpose share 3 and share 4, after superimposing these shares we get the 2nd quadrant of original image.

Step3: We superimpose share 5 and share 6, after superimposing these shares we get the3rdquadrant of original image.

Step4: We superimpose share 7 and share 8, after superimposing these shares we get the 4thquadrant of original image.

Step5: after stacking the entire relevant share with each other we retrieve the original image that we have divided into 4 quadrants.

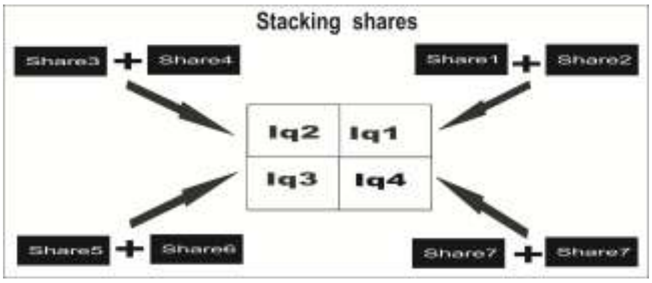

Fig 2.2

Purposed technique pictorial overview:-

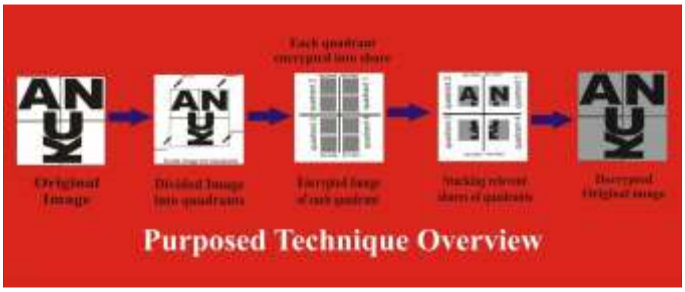

Fig 2.3

3. Practical Implementation of Proposed Technique.

Steps 1 We have an original Image I as shown Fig 2.1

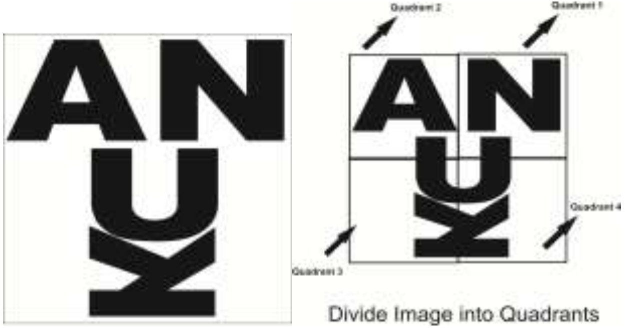

Fig 2.1 Fig 2.2

Step:2 Divide the original image into 4 quadrants as shown Fig 2.2.

Step 3 Apply (2, 2) secret sharing Encryption to quadrant 1 shown in Fig 2.3

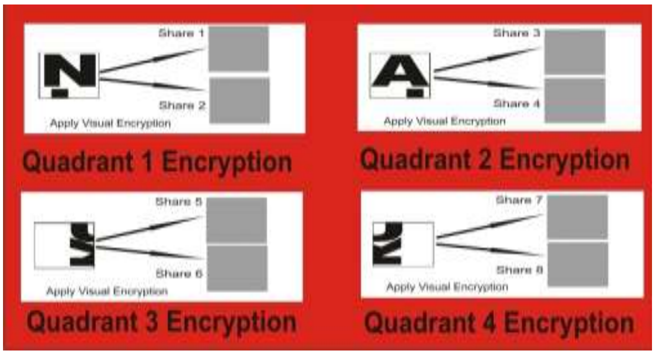

Fig 2.3

Step 4 Apply (2, 2) secret sharing Encryption to quadrant 2 shown in Fig 2.3

Step5 Apply (2.2) secret sharing Encryption to quadrant 4 shown in Fig 2.3

Step6 After applying Visual Encryption to the quadrants the resultant shares we get are shown in Fig 2.4

Decryption

Step 1: Stack the shares of 1st quadrant (i.e. Share 1& Share 2) and we get image of 1st quadrant

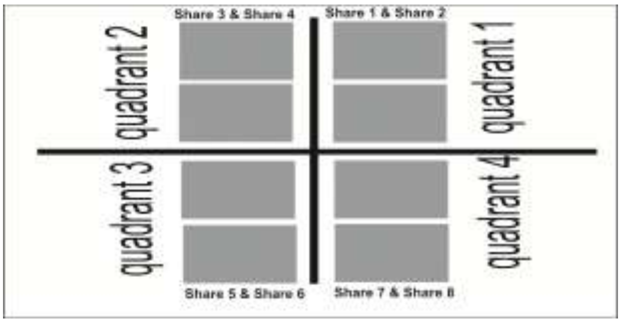

Fig 2.4

Step 2: Stack the shares of 2nd quadrant (i.e. Share 3& Share 4) and we get image of 2nd quadrant as shown in Fig 2.5.

Step 3: Stack the shares of 3rd quadrant (i.e. Share 5& Share 6) and we get image of 3rd quadrant as shown in Fig 2.5.

Step 4: Stack the shares of 4th quadrant (i.e. Share 7& Share 8) and we get image of 4th quadrant as shown in Fig 2.5.

Step5: Now manually combining all resulting images of the quadrants which we have get form stacking the shares.

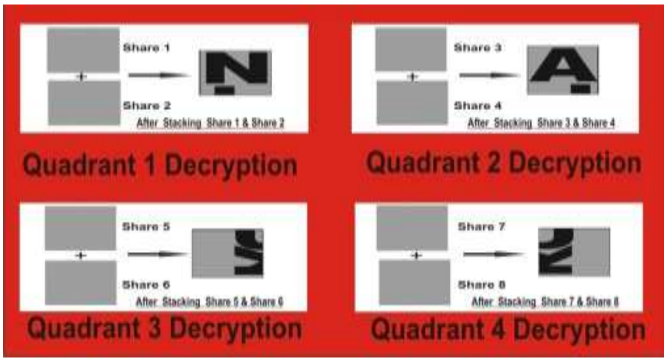

Fig 2.5

Step6: In this final step we get the original image as shown in fig 2.6

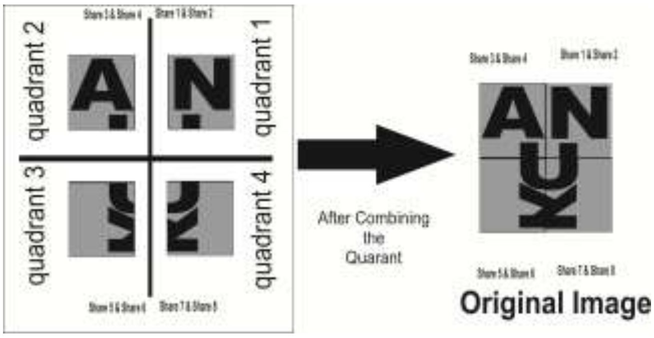

Fig 2.6

4. Conclusion

By using the proposed method we can encrypt the image with high level of security even by using simple (2, 2) secret sharing scheme. The proposed method is faster than other schemes because it follow simple (2, 2) secret sharing scheme which generate only two share for encryption and required only these two shares for decryption.

All shares are required to regenerate the original image, missing of any share will not result in the reveling the original image. We can also increase the security just by increasing the number quadrants of image.

5. Future Work

The present work is concern to code a program in which division, encryption and decryption are performed in different modules, which increase the complexity of the proposed technique. Further research in this technique allied to the present study is suggested below:

1) To code a program which division, encryption and decryption are performed in a single program.
2) To study the impact of image size in the proposed technique
3) We will also implement the following method for the audio encryption.

References

[1] Sumedha Kaushik & Ankur Singhal "Network Security Using Cryptographic Techniques" Volume 2, Issue 12, December 2012, IJARCSSE.

[2] Shamir, How to share a secret, Communications of the Association for Computing Machinery, vol. 22, no. 11, pp. 612-613, 1979.

[3] Sonali Patil1, Sandip Sathe2, Pravin Mehetre3," Secure and Verifiable (2, 2) Secret Sharing Scheme for Binary Images" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 2, January 2013

[4] Suman Chandrasekhar, Akash H.P, Adarsh. K, Mrs. Smitha Sasi"A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem" Volume 11, Issue 2 (May. - Jun. 2013), IOSR-JCE.

[5] Yogesh Kumar, Rajiv Munjal,Harsh Sharma "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" Vol. 11, Issue 03, Oct 2011, IJCSMS.

[6] Pratap Chnadra Mandal," Superiority of Blowfish Algorithm", Volume 2, Issue 9, September 2012 ISSN: 2277 128X, IJARCSSE.

[7] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt 94, pp. 1–12, 1995

[8] Shamir, How to share a secret, Communications of the Association for Computing Machinery, vol. 22, no. 11, pp. 612-613, 1979

[9] Bibhas Chandra Dhara , "k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence", IJCA (0975 8887)Volume 25–No.11, July 2011

[10] Jayanta Kumar Pal, J. K. Mandal2 and Kousik Dasgupta, "A (2, N) VISUAL CRYPTOGRAPHIC TECHNIQUE FOR BANKING APPLICATIONS" International

[11] Shyamalendu Kandar & Bibhas Chandra Dhara, "k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence" IJCA (0975 8887)Volume 25–No.11, July 2011

[12] Abhishek Kr Mishra, Ashutosh Gupta & Ashish Kumar , "(n, n) Visual Cryptography based on Alignment of Shares" IJCA (0975 – 8887) Volume 60– No.18, December 2012

Author Profile

Ankush Sharma received the B.Tech degree in Computer Science Engineering from GHEC, Solan (H.P.) in 2010. After that he worked as lecturer in MIT, Bani, Hamirpur (H.P.) for one year. He is now as a research scholar in Carrer Point University Hamirpur (H.P.).

Aarti Devi received the B.Tech degree in Computer Science Engineering from IEET, Baddi (H.P.) in 2011. After that she worked as lecturer in Gautam Girls College Hamirpur (H.P.) for six months. She is now as a research scholar in Carrer Point University Hamirpur (H.P.).

Anamika Rangra received the B.Tech and M.tech degree in Information & Technology from JAYPEE University, Waknaghat, Solan (H.P) in 2012 and 2014. She had been two research paper published in security in Cloud Computing. She has a IEEE Membership. She is now as a Assistant Professor in Carrer Point University Hamirpur (H.P.).

Gandharv Singh received the Bachelor in Computer Application degree from Netaji Subash Chand Bose Memorial Collage Hamirpur (H.P.) in 2009 and he did Masters in Computer Application from DIM kurukshetra. After that he worked as a php developer in infomatics Mohali for one year. He is now as a research scholar in Carrer Point University Hamirpur (H.P.).