International Journal of Engineering & Technology, 7 (3.34) (2018) 810-812

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Visual Cryptographic Mechanism for Secret Information Sharing

Prasanna Kumar H.R,Dr. Niranjan N. Chiplunkar

Research Scholar, NMAMIT, Nitte, Karnataka, India
Principal, NMAMIT, Nitte, Karnataka, India
*Corresponding Author Email: *hrpbhat@gmail.com* , *niranjanchiplunkar@rediffmail.com*

Abstract

Security and confidentiality aspects are very much essential for sharing secret information. To provide security to the information conventional encryption technique may be used; which requires high computation and the security is also not in acceptable level. The quality of input image and the recovered image is same. The other approach involves use of visual cryptographic techniques where shares are created for the secret images and the recovered image quality is an issue. We proposed a method for transferring confidential image, which make use of two stages during encryption. Instead of sending the confidential image directly to the receiver, send an encrypted form of the image along with three shares. During decryption decrypt the encrypted image using random numbers and flag values. The proposed method provides multi- layered security for transmitting the confidential image.

Keywords— Cryptography, Security, Random numbers, shares, Multi layer security

1. Introduction

Security has become an important and major problem and avoiding access of confidential data by the intruder has been challenging task [1]. Day by day due to the extensive growth in wireless communication and development of network, people can access the internet by cell phones and computer. Individuals put huge volume of images or video online for various purposes. These images or video may contain secret information or private data [2]. Because of fast advances in communication and information technology, the data is kept electronically, so that the security has turned into a principal issue. Privacy and data integrity are especially required to secure the information against unauthorized persons, who are trying to get the secret information. The users use more information by downloading the document from the source of internet and sometimes they must upload the source of information to the digital media. Here the data or the information ranges from simple text, photos, records, documents to all other multimedia data. Due to the technology of internet it provides very easy way of access to other data or the information. Hence there is a huge demand for protecting this visually available information from unauthorized person and also making of duplicate copies of the same information by the theft.

To transmit confidential data like military information, financial documents, Internet become the major and primary source [3]. Many of the digital images which contain confidential data are transmitted through the internet but it is not secure [4]. Now a day, it is difficult to trust the secret data or information available on the internet, [5] due to uncontrolled hacking on the internet [6], therefore while transferring confidential images, security aspects are essential for consideration, since the intruders may make use of weak links in the communication path of the network, to get information that they required [7]. While transmitting secret data, maintaining the privacy of data and security has become the major issues [8].

Cryptography is the method used to protect messages which are sends through the e-mails, information about credit card and data related to corporate. Cryptography is a method of protecting information that is confidential. Cryptography is the widely used method, which overcomes the threat by the intruders. Cryptography involves mathematical functions and it converts secret input into cipher code. Cryptography is used to store information that is sensitive or transmit it through insecure communication channel so that it cannot be identified by anyone except the trusted recipient.

Cryptography systems are of two types. In symmetric method, same key is used for both encryption as well as decryption. Two keys are required in asymmetric key cryptography [9]. In this approach, encryption requires one key and the second key is used for decryption. In symmetric key cryptography, sender and receiver share the key secretly [10]. Utilizing the joint key, sender can encode the information and afterward transfer it to the receiver. In public key cryptography or asymmetric method, two different keys are used for encoding and decoding process [9]. This technique requires every client to have two keys-a private key and public key. The sender, who needs to send confidential data, encodes the message by utilizing the beneficiary's public key. The recipient utilizes his private key to decode the message. The original secret message is called plaintext, which is in readable form. The encrypted message is called cipher text, which is scrambled message. In public key cryptography, a public key is known to everyone and two keys are mathematically related. Obtaining private key value is computationally infeasible from the public key, in public key system.

In symmetric method, the security of data is dependent on the

security of the key. The advantage of symmetric cipher is that it executes faster and the method is less complex. In symmetric approach, key should be shared securely among the participants. But in public key method, sharing of key is not required. Compared with symmetric approach, asymmetric method is slower, but it is more secure [10].

The approaches proposed earlier to encryption and decryption had their own limitations like high computation cost and key management. These problems create a motivation to develop encryption and decryption process for an image to provide an authentication without using a key [11]. Encryption of images using some traditional encryption techniques like DES, RSA are not suitable due to the correlation property and bulk storage of the image.

Keeping the main objective of converting information into unreadable ciphers, many cryptographic algorithms have been developed .The two methods being applied for images to maintain the confidentiality [12]. The first method is similar to conventional encryption technique; it requires both secret key as well as an encryption algorithm. Here key management is the major issue. The drawback is that it requires high computation and the security is also not in acceptable level. The major strength of this method is that, the quality of the recovered image is similar to that of original image. The second approach involves dividing the secret image into many shares, and we cannot reveal any secret information from those shares. Only the set of qualified shares are considered to obtain original image [13]. The main issue of this approach is that the quality of recovered image is not good. Managing the key is not required in this method and is the major strength of this approach. The paper contains the following sections: Section 2 discussed about the existing system. Section 3 gives the proposed method, which contains the architecture, encryption algorithm, share creation and decryption process. Results of the proposed method are discussed in section 4.

2. Existing Works

The secret image is initially encrypted using intensity variation technique and then encrypted using pixel swapping algorithm [14]. During intensity variation step, corresponding to each color in a pixel, the method generates three random numbers [15]. Also it maintains three flag values to do this operation. Pixel swapping method is referred as single swap per each pixel, because every pixel swapping takes place only one time [14]. The random values of each pixel are considered for pixel swapping. During encryption and decryption, flag values and random values are considered as key. For achieving better security, flag values and random values are converted into image [14]. Three shares are generated by considering random values and flag values [14]. The sender sends the encrypted image and three shares to the receiver. Decryption process is exactly the reverse of encryption. Binary Image Visual Cryptography [16] Visual Cryptography allow us to share secret effectively and efficiently, the secret image can be distributed in to two or more shares, when shares are superimposed exactly together the original image would be discovered with human visual system(HVS) without out aid of computer or without performing complicated computations.

3. Proposed Method

In the proposed method, secret image is considered as an input image. In the first step of encryption process, intensity variation technique is applied for the input image. During the second step of encryption process, pixel swapping method is applied. Three different techniques are applied for pixel swapping. Shares are created by using random numbers and flag values, which are generated during intensity variation step of encryption. Two different methods are applied for creating the shares. During decryption, any of the three swapping method is applied and then decrease the intensity of pixel to get the original image. The quality of the recovered image is same as that of original secret image. The original confidential image is considered as input. Two levels of encryption have been applied by swapping the pixel and by increasing the intensity level. The flag values, random numbers and encrypted image are output for this stage. By considering flag value, random numbers, three shares are created using two different techniques. The three shares along with encrypted image are sending to the receiver for decryption. During decryption, flags and random numbers are extracted from three shares and decryption process is applied for encrypted image to obtain original confidential image.

The original secret image is considered as input and is encrypted in two levels by varying the pixel intensity and swapping the pixel values. Pixel intensity of each pixel is changed accordingly to the random numbers generated. Generate three random values and three flag values for each pixel. While adding random value to corresponding color factor if it exceeds 255 then random value is not added, otherwise it is required to add random value. If color factor is increased by adding random value then flag value of that color is set, otherwise it is not required to set the flag value. In the second level of encryption, pixel value is interchanged using any of the three algorithms. The algorithm for proposed iterative swap method is shown below:

Algorithm Iterative-swap (Secret-image M)

For each pixel x in the image M do

Begin

Sum = r1 + r2 + r3 // r1, r2, r3 are three random numbers used for pixel x

If ((Sum mod 3) = 0) then

Swap the pixel values with the corresponding pixel in the other end of same row

Else if (Sum mod 3) = 1

Swap the pixel values with corresponding pixel in the other end of same column

Else

Swap pixel value with corresponding pixel in other end of diagonal

End if

End

In the second method, divide the image into four equal blocks. In the second method, divide the image into four equal blocks and do the operation according to the following algorithm.

Algorithm Swap-halfpixel (Secret-image M)

Divide the image M into four equal blocks b1, b2, b3 and b4

For each block do

Begin

Divide the block into four equal sub division d1, d2, d3 and d4

End

In the third method, divide the secret image into four equal blocks and apply the method of swapping for each pixel of each of the block separately to obtain encrypted image and random numbers [14].

Two methods are applied for creating shares; additive method and factor method. Flags and random numbers are the input for share creation phase. In the factor method, random value of blue is

divided into three factors and each factor is set as value for blue factor in all three images. The similar process is repeated for green and red accordingly. For alpha value of all three images sum of all flag values of blue, green and red are assigned. To get back the random values and flag values from shares, need to collect color factors from all three images, which give the required information. In case of random number of blue, we need to multiply all three blue factors from three shares, similarly for red and green. Encrypted image is decrypted in two steps. In the first step, pixel values are interchanged using any of the three methods. In the second step, vary the pixel intensity to get back the original image.

4. Results and Discussion

In the proposed method, image which is considered has to undergo encryption so that the intruder does not come to know that the secret image straight forwardly. Whatever data is used to encrypt the image are also created as an image and is sent to receiver. Random values used to encrypt the image differ every time the application is run. All images along with encrypted image are sent to the receiver and the concerned person should be well aware of the algorithms used for encryption so that he can decrypt it and get back the original information. Fig 1 show encryption process using iterative swap method as mentioned in the section 3 and Fig 2 show the shares generation phase to provide the security to the secret image. Fig 3 shows the decryption procedure to obtain the original encrypted image.

Fig 1: Encryption using iterative swap

Fig 2: Share creation using additive method.

Fig. 3: Decryption process.

5. Conclusion

A practical, computationally cost-effective and visual cryptographic mechanism is proposed for secret information sharing. In the proposed method, confidential image is encrypted using two phases to increase the security level. In the first phase, intensity of each pixel is changed accordingly to the random numbers generated. During the second phase, change the color value of each pixel using three different algorithms. The encrypted image along with three shares is send to the receiver. During decryption, flag and random values are extracted from three shares and are used to get original secret image. Due to two phases during encryption, the proposed method provides high security for confidential information. Instead of sending random numbers and flag value directly to the receiver, create three shares and send the shares to the receiver. This gives another layer of security to transfer the secret information. The proposed method provides high security and it gives the better quality decrypted image.

References

[1] J. K.Mandal, SubhankarGhatak, “A Novel Technique for Secret Communication through Optimal Shares Using Visual Cryptography”, International Symposium on Electronic System Design (ISED), 2011, pp. 329-334

[2] J. K.Mandal, SubhankarGhatak, “Constant Aspect Ratio Based (2, 2) Visual cryptography Through Meaningful Shares”, International Conference on Communication and Industrial Application (ICCIA), 2014, pp. 1-4

[3] Jaya, Siddharth Malik, AbhinavAggarwal, Anjali Sardana, “Novel Authentication System Using Visual Cryptography”, 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, 2011

[4] John Justin M, Manimurugan S, Alagendran B, “ Secure Color Visual Secret Sharing Scheme Using Shifting Coefficient with No Pixel Expansion”, International Journal of Computer Science and Information Technologies, Vol. 3(2), pp. 3793-3800, 2012

[5] Chetana Hegde, “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”, Proceedings of the 16th International Conference on Advanced Computing and Communications, 2008

[6] MoniNaor, Adi Shamir, “Visual cryptography”, Advances in Cryptography, Eurocrypt’94, Lecture notes in Computer Science, Springer-Verlag, Vol. 950, pp. 1-12, 1995

[7] Young-Chang Hou, Pei-Hsiu Huang, “Image Protection Based on Visual Cryptography and Statistical Property”, IEEE Statistical Signal Processing Workshop, pp. 481-484, 2011

[8] John Blesswin, Rema, Jenifer Joselin, “Recovering Secret Image in Visual Cryptography”, International Conference on Communications and Signal Processing(ICCSP), IEEE Conference Publications, 2011, pp. 538-542

[9] Warjri, Janailin, E. George Dharma Prakash Raj, “KED-A Symmetric Key Algorithm for Secured Information Exchange Using Modulo 69”, International Journal of Computer Network and Information Security, 2013

[10] J. Ramya, B. parvathavarthini, “An Extensive review on Visual Cryptography Schemes”, Proceedings of the IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, pp. 223-228

[11] Wei-QiYan, Duo Jin, M.S. kankanhalli, “Visual Cryptography for Print and Scan Applications”, Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS’04), Volume 5, 2004, pp. V-572-V-575

[12] Jaya, Siddharth Malik, Anjali Sardana, Jaya, “A Keyless Approach to Image Encryption”, Proceddings of the International Conference on Communication Systems and Network Technologies, 2012

[13] Alharthi, Saeed s, pradeep K. atrey, “Further improvement on secret image sharing scheme”, Proceedings of the 2nd ACM workshop on Multimedia in forensics security and intelligence, 2010

[14] Shetty Deepesh Sadananda, Anusha Karkala, “Image Encryption and Decryption Using Image Gradient Technique”, International Journal of Emerging Technology and Advanced Engineering, Volume. 3, Issue. 1, January 2013. Pp. 511-515

[15] Liguo Fang, BinYu, “Research on Pixel Expansion of (2, n) Visual Threshold Schemes”, 1st International Symposium on Pervasive Computing and application, pp. 856-860, 2014.

[16] Yaseen Hikmat Ismaiel, Muna Mahmood Khether, “Binary Image Visual Cryptography”, Vol. 177, No. 6, November 2017.