Cryptographic Techniques for Data Security and their limitations

Abhishek Goyal, Alok Goyal, Parag Bhavsar, Nadeem Kapshikar

Abstract— Cryptographic techniques have long been used for secure communication of secret messages across an unsecure medium. The message in plaintext is encrypted, to keep the information safe and secure from prying eyes. In Steganography the secret message or information to be secured is hidden in a multimedia file (generally an image file) in such a way that there is no noticeable change in the appearance (in case of an image file) or working (in case of sound file) of the original file. Visual Cryptography is yet another cryptographic technique which is used for securing the image files by dividing the image in 'n' shares such that no individual shares can reveal the data, but when the shares are stacked on top of each other, the hidden data is revealed. Although many different algorithms and techniques have been developed for each of these cryptographic algorithms the secrecy of data is still not guaranteed. There have been various instances where these methods or some variations of them have been broken and the security of data been compromised. In this paper we review the traditional methods of securing data and their limitations. In the end we propose to develop an algorithm for secure transmission and sharing of images across an unsecured medium by combining all these three techniques and its applications.

Index Terms— Cryptography, Encryption, Decryption, Data security, Image scrambling, Steganography, Visual Cryptography

1 INTRODUCTION

We live in a highly connected world today and in today's information age digital data security is of paramount importance. From communication to banking to shopping, we do almost all of the stuff online today. We transfer and share a lot of our personal data with other people over the network. This sensitive information needs to be secure and should only be accessible to those for whom it is intended. Unauthorized access to our personal information or data should be blocked. To provide this security and safe communication channel, cryptographic techniques are being used. Cryptography refers to the technique of modifying the original message (plain text) in such a way that it appears random or useless (known as cipher text) to any third party or intruder who intercepts it. Only the persons who know the key or method can convert the message back to plaintext and get to the original message. There are numerous cryptographic algorithms and different techniques that have been developed to ensure the security of data but still are not secure enough and there have been many instances of data being compromised due to some weakness in the above methods. In this paper we discuss the various approaches used to ensure data security and their limitations and propose a new method for security of digital images and its applications.

- *Abhishek Goyal is currently pursuing bachelors degree program in computer engineering in MIT College of Engineering,Pune, India, PH-091-7276755691. E-mail: abhishek.goyal9419@gmail.com*
- *Alok Goyal is currently pursuing bachelors degree program in computer engineering in MIT College of Engineering, Pune, India , PH-091-8149253471. E-mail: alokg1019@gmail.com*
- *Parag Bhavsar is currently pursuing bachelors degree program in computer engineering in MIT College of Engineering, Pune, India , PH-091-8149463426. E-mail: paragbhavsar44@gmail.com*
- *Nadeem Kapshikar is currently pursuing bachelors degree program in computer engineering in MIT College of Engineering, Pune, India , PH-091-8149626946. E-mail: nadimkapshikar786@gmail.com*

2 CRYPTOGRAPHY

Cryptography deals with the process of converting a plaintext message to unreadable cipher text. The cipher text looks random and useless. The process of converting the plaintext to cipher text is known as encryption and the reverse process is known as decryption. A very basic method for encrypting messages is by shifting the alphabets by certain number of positions(key) is known as Caesar cipher. It is one of the first algorithms used for encryption. Later many different algorithms have been proposed which are better and provide far better security than early substitution ciphers. Also a number of approaches have been developed against the substitution ciphers such as frequency analysis, which greatly reduce complexity in breaking these algorithms. Modern day cryptography uses complex mathematical computations to encrypt the original message in such a way that it is very difficult to break these methods, although not impossible.

Modern cryptographic techniques can be divided into two groups: Symmetric Key cryptography and Public key cryptography. In symmetric key, method sender and the receiver share the same key for encryption and decryption of the message. For this there is an additional need for both the parties to be able to share the key in advance before using it for communication. The security of the message using this scheme depends upon the security of the key.

Public Key Cryptography is also known as asymmetric key cryptography. In this method two different keys are used for encryption and decryption of the message. There are two set of keys for each of the sender and receiver known as public key and private key. The public key can be freely distributed to everyone while the private key is kept safe and is not shared with anyone. The message encrypted using a public key can only be decrypted using the corresponding private key. The sender sends the data by encrypting using the receiver's public key. The receiver can then decrypt the data using

its private key which is known only to the receiver. Similarly the receiver can send data to the sender using the sender's public key which can only be decrypted with the sender's private key which is only know to the sender.

These techniques however involve very complex mathematical calculations and require more computation power. Although these techniques can be used for text as well as image or other media files, the large size of the multimedia files makes use of these algorithms inefficient and may considerably slow down the system due to very large number of computations required for these files. There is therefore a need to develop a simple algorithm which provides the same level of security as these algorithms provide and also does not slow down the system performance.

3 STEGANOGRAPHY

Steganography deals with the practice of covering a message, image, or file within another message, image, or file. The words steganos meaning "covered, concealed, or protected", and graphein meaning "writing "together form a single word steganography. Steganography is different from cryptography. Cryptography means doing alteration in original data whereas stegno means concealing the encrypted data into another form so that observer cannot view the data. Thus it is an "invisible" communication. Steganography sometimes is used when encryption is not permitted or recently, steganography is used to supplement encryption. An encrypted file may still hide considerable amount of information using steganography, so even if the encrypted file is decoded, the hidden message is not seen. The main advantage of steganography over cryptography is that it hides the existence of data. Even if an intruder is able to gain access to a particular file, he may not be aware of the concealed file or data which may be hidden in the innocent looking and completely unrelated file. The most common form of steganogrpahy which is used is image steganography. In this technique a text message or a data file may be hidden in an image file without distorting the look of the original image.

An interesting concept implemented by Mohamad Shirali-Shahreza [7] is steganography in multimedia messaging. This method presents hidden communication using text and image stenography. He talks about hiding data in text message or in SMS or in MMS by basic concept called abbreviation. He uses expression like 'k' instead of 'okay' or 'u' instead of 'you'. He then hides some of the information data in text as well as some data bits in images. However, this method is easy to attack as it is simple to search for possible abbreviations.

A more secured technique is given by Piyush and Paresh Marwaha[8] in which they combined cryptography with stenography for more secured implementation. They use a reference grid(3-D database) in which R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. They proposed that for every character in a message a specific and unique change will be made in their RGB value. This change of bits will be dependent on data position selected from (grid) reference database. To decrypt the same receivers private key is used to identify reference (block no) from the reference database. The difference in pixel value gives the decrypted text. The method is proposed only for the jpeg images and not for images in other format limiting its scope.

4 IMAGE SCRAMBLING

Image Scrambling is defined as reordering the image, usually the position bits/pixel of image so that people or computer system cannot perceive the true meaning of original image. Most of the algorithms try to create a chaotic image to hide the original content of the original image. Several methods have been proposed since the inception of this idea, to scramble a given image as discussed below.

[1]HB Kekre, Tanuja Sarode, Pallavi Halarnkar in august 2013 suggested a matrix transformation method called Relative-Prime Shuffling method in which is based on the size of image(M*N) they find out all relative prime numbers and save it in set S. Using this set S they finds correlation between first row and remaining row, considering the lowest correlation as a key to shuffle the rows in the image, saving all relative number as a key for row/column shuffling[1] can then be use to decrypt the original Image back. The Major Disadvantage of this Method is we have to convert the color image to Gray Scale Image and it is very hard to again convert Gray scale to Color Image.

A new parameter based M-sequence which can be produced by a series shift registers is introduced in [2]. In this paper a new image scrambling algorithm is introduced based on M-sequence. The user can have some security keys r which give the number of shift operations to implement and parameter k which is distance parameter to generate M different encrypted sequence. Thus this algorithm provides extra security with its key based technique. It makes difficult to decrypt the scrambled images thus providing better security performance than other it can encrypt the 2-D and 3-D images in one step. It has better result and performance with filters and noise attacks

[3] Lianyuan Jiang, Haohao Yuan in 2014 suggest a new method based on Grouping Calculation. This algorithm Divides every byte of stored image information into three groups and swaps the position of each group so that pixels are scrambled and then calculating the value of three group using new byte calculation formula so that now pixels color value are scrambled. This algorithm shows a satisfactory Scrambling result. The main disadvantage of this method is it has many complex calculations.

Tang et al., [4] propose an image scrambling algorithm that needs no iterative calculation. This algorithm divides bits of each pixel into even and odd groups. Those in the even group are swapped so that the original higher bits become lower and vice versa. Shao el al [5] proposed a more improved scrambling method based on avalanche. Image Scrambling transformation that scrambles the original image through inverse

transformation and recovers the scrambled image through obverse transformation.

Another Method Described by Prashan Premaratne from University of Wollongong in 2012,[6] titled "Key based Scrambling for secure image communication" which take a key(a number) and calculate the new value using module method. I.e if the size of image is 256*128 (256%key_value) is your row value and (128%key_value) is your new col value, just swap the new row with col value. The key must be store in some file(metadata) which is used to descramble the image. The disadvantage with this method is again extra space is needed to store the key value, but it provides a better security than other method.

5 VISUAL CRYPTOGRAPHY

Visual Cryptography is a special type of encryption technique to obscure image based secret information which can be decrypted by human visual system. This cryptographic system encrypts the secret image by dividing it into n number of shares and decryption is done by superimposing a certain number of shares(k) or more. This method is different from traditional cryptographic methods because it requires no complex calculation or computation for decryption process and the original image become recognizable to the human eye without any computations when the shares are stacked on top of each other. The original method was proposed by Naor and Shamir for monochromatic images [9].

Earlier visual cryptography was only limited to monochromatic images only (black and white mostly) and this approach was not efficient as the shares generated were of bigger size than the original image and the recovery process was also not efficient because the recovered image has less contrast than the original image and the size of the recovered image was bigger. The drawback of this method was reduced contrast, increased image size and limited to monochromatic images. Later on several different variations of the algorithm were proposed mostly for monochromatic images.

Blundo had proposed an optimal contrast k-out-of-n scheme to alleviate [10] the contrast loss problem in the reconstructed image.

Later on the concept of VC was been extended such that the secret image is allowed to be a greyscale image rather than a binary image. Although the secret image is greyscale, shares are still constructed by random binary patterns. Nakajima extended EVC to a scheme with natural greyscale images to improve image quality [11].

The limitation of all the methods lies in the fact that all shares generated are random patterns carrying no visual information. There are some approaches to colour VC as well, which attempts to generate meaningful shares but it produces shares with low visibility due to colour inconsistency across colour channels.

In [13] a method for visual cryptography on colour images is proposed in which the original image is divided into C, M, Y shares. These shares are then divided into 2 shares by traditional method proposed by Naor and Shamir. C gives C1 and C2, M1 gives M1 and M2, Y gives Y1 and Y2. Then 2 more share are generated by combining C1,M1 and Y1 other share by C2,M2 and Y2.The disadvantage of this algorithm is that for single image many shares are generated and due to using traditional algorithm for splitting image the size of the shares increases.
RKO [12] technique is one of the most efficient algorithm for dividing image shares for colour images. In share 1 random pixels are taken and other share is generated by XORing share 1 and original image. This gives share 2 .These two shares are completely random and original image cannot be recovered using only one of the shares. XORing both the shares gives the original image back without any change in quality. The problem with this algorithm is it is not very secure as simple XOR operation is used, which if broken, can reveal the image easily.

Our objective is to add more security to images so that it does not get easily decrypted and in our opinion each share should also be meaningful and contain some information.

The main principles of visual cryptography are not storing the information in a single place and decryption using simple computations.

5 CONCLUSION

In this paper we have discussed the traditional approaches used for the security and integrity of data and the different algorithms which are available for them. Still these are not sufficient enough to provide adequate security by using any of these alone. We therefore propose to develop an algorithm for secure storage and transfer of images by using the basic principles of visual cryptography along with traditional cryptography, steganography and image scrambling techniques. The algorithm will be simple enough and not involve complex computations and at the same time be robust enough to provide adequate security to images.

If the algorithm is fast enough that it takes minimum computation, it can also be used in web applications to securely store and transfer images files without being compromised. Currently all the image files for a website are accessible to all if one has the link of the image. Even the private images are not private in the true sense as we just hide the complete link of the image file and not the file itself. Eg: Social networking sites like Facebook have an option of securing images by making them private. However they do not actually block access to the image files. All that is done is the link of the image file is not accessible to everyone, instead only to a select few people who have been given permission. If anyone one of them copies the link of the image and circulates it or opens in the browser, the supposed private image will be openly accessible to everyone even without logging in the Facebook account, as Facebook

stores the image files on a separate CDN server. The image files are not given the security and privacy they should be given, as the current methods for encryption are either costly in terms of performance or cannot be used for the above scenario.

If the images can be secured by minimum amount of computation then the above mentioned problem could be solved, which we aim to achieve by developing the proposed algorithm. In this way the security of the image or digital data could be greatly increased. As there is no single point of failure this system will be more robust and largely secure than the traditional systems which provide single line of defence.

REFERENCES

[1]. H B Kekre1, Tanuja Sarode2, Pallavi Halarnkar3,Image Scrambling using R-Prime Shuffle,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,Vol. 2, Issue 8,August,2013

[2].Yicong Zhou, Karen Panetta, Sos Agaian, ,An Image Scrambling Algorithm Using Parameter Based M-Sequences,, In Proc International Conference On Machine Learning And Cybernetics, 2008 (Volume:7), Pp 3695 ,Äì 3698,July2008

[3]. Lianyuan Jiang1,2, Haohao Yuan1, Jianbing Jiang1, Yalan Zhang1 and Jian He1,Image Scrambling Algorithm based on Grouping Calculation,International Journal of Security and Its Applications Vol.8,No.3(2014),pp.209-220

[4]. Z. Tang, X. Lu, W. Wei and S. Wang, ,Image scrambling based on bit shuffling of pixels,, Journal of Optoelectronics.Laser, vol. 18, no. 12, (2007),pp.1486-1488,1495.

[5]. L. Shao, Z. Qin, X. Heng, H. Gao and X. Wang, ,ÄúAvalanche image scrambling transformation based on high-dimension matrix transformation,Äù, Journal of Image and Graphics, vol. 13, no. 8, (2008),pp.1429-1436.

[6]. P. Premaratne , M. Premaratne, "Key-based scrambling for secure image communication," in Emerging Intelligent Computing Technology and Applications, P. Gupta, D. Huang, P. Premaratne & X. Zhang, Ed. Berlin: Springer, 2012, pp.259-263.

[7]. M. Shirali-Shahreza, "Steganography in MMS," in Multitopic Conference, 2007. INMIC 2007. IEEE International, 2007, pp. 1-4

[8]. Piyush Marwaha, Paresh Marwaha , VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES,2010 Second International conference on Computing, Communication and Networking Technologies

[9] M. Naor and A. Shamir, “Visual cryptography,” in Proc. EUROCRYPT’ 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS

[10] Carlo Blundo, Annalisa De Bonis, Alfredo De Santis,Improve Schemes for Visual Cryptography,Designs, Codes and Cryptography, December 2001, Volume 24, Issue 3, pp 255-278

[11] Mizuho Nakajima, Yasushi Yamaguchi,"Extended Visual Cryptography for Natural Images”

[12] Ms. Moushmee Kuri1, Dr. Tanuja Sarode2,"RKO Technique for Color Visual Cryptography",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 89-93

[13] Joshi Jesalkumari A., R.R.Sedamkar, Modified Visual Cryptography Scheme for Colored Secret Image Sharing, International Journal of Computer Applications Technology and Research Volume 2– Issue 3, 350-356, 2013