AN EFFICIENT APPROACH FOR SECRECY BY SDS ALGORITHM

[1]Anisha K Jose, [2]Panchami V

[1]Postgraduate Student,Toc H Institute of Science & Technology, Kochi
[2.] Assistant Professor, Toc H Institute of Science & Technology, Kochi

ABSTRACT

Security of data and image has grown and evolved significantly in recent years. Mainly two approaches are used for security. The first approach involves encryption of images and data through encryption algorithms using keys. But there exist the problem of heavy computation and key management. The second approach involves dividing the image into random shares to obtain image secrecy. But it also has the problem of less quality of the recovered image at the time of decryption. So a novel approach without the use of any encryption key is proposed in this paper. Main objective of the proposed system is to obtainthe confidentiality and authenticityofboth data and images. The major steps involved in this approach are Filtering, Division and Shuffling to create random shares such that with less computation, the secret image can be reconstructed from these random shares without any loss of image quality. The total numbers of shares aredetermined using random number generation technique.Data encryption can also be done by converting the data into an image. This project will provide a system to serve both sender and receiver of the secret message. To provide more security to the data, the authenticated entity will keep the fingerprint of the original receiver. After the fingerprint authentication, the secret image is transmitted to the authenticated receiver. This transmission can be done in the wireless sensor network by any data transmission technique.

Key words: Image encryption, Fingerprint, shuffling.

INTRODUCTION

Today's communication technology becomes obsoletefor tomorrow's necessity. The growth of the communication industry is unimaginable. The emergence of internet introduced

to its users a new dimension called sharing of data in real time. Now a day's people are familiar with sharing of data from one side of the world to the other side in real time. But along with these opportunities there are certain challenges that are how to maintain the secrecy of data. It is the time for providing internet services in an undisturbed way. So a new sparkling area of research evolved in the field of cryptography called encryption. There are so many traditional encryption techniques RSA, AES, DES etc.But they are also facing certain difficulties. Even the most popular 56 bit key DES algorithm [11] is broken by two famous American scientists and they won a million dollars as price. So the technology has to be updated every day to meet the requirements of various industries. Likewise there are so many encryption algorithms are there. And each of the encryption techniques has its own advantages and disadvantages. It is now a challenge to provide the flow of information seamlessly without any modification of data. This paper discusses the methodology of providing secure data transmission of data and images. Cyber security is a primary concern in today's environment. A reliable, secured data transmission does not allow hackers to snoop into others data. Thus data hacking is not possible if the encryption algorithm used here is implemented.

Recent days visual cryptographic schemes are used in a wide range.This gave rise to a new area of research for image encryption. Encryption of images is mainly of two types. That is lossless and lossy image encryption. This classification resulted in two different lines of approaches being adopted for maintaining confidentiality of images called image encryption and image splitting.Image Encryption is typically similar to the conventional encryption methods which involved using an algorithm and a key to encrypt an image. Some of the techniques for encrypting images are "Vector Quantisation", "Chaos Theory" [2], "Visual Cryptography" etc. There are certainproblems with these techniques; they involve secret keys and thus have all the limitations of keymanagement. In addition, in some cases there is a problem of restricted key space. Also computation cost involved in encryption is high. There is also the issue of week security. However the greatest strength of most of these schemes is thequality of the recovered image.

Image splitting, involves splitting an image at the pixel level into multiples shares, such that individually the shares reveal no information about the image, but a selected set of these shares will help regenerate the original image for partially. Adi Shamir [6] in 1979

proposed the idea of dividing a secret data into 2 random shares. In1995, Naor and Shamir, proposed the new encryption scheme "Visual Cryptography"[7], that involves sharing of a secret image by dividing it into multiple shares. Many variations to the scheme are proposed to overcome the limitations, each having their own advantages and disadvantages. In spite of the advancements made in this line of research, the quality of the recovered s images still remains an area of concern due to the low quality of these recovered images; including loss of contrast and colours.In spite of its limitations the greatest strength of these schemes is that firstly, there is no key management problem and secondly the process of recovery of real image involves no computation. To overcome the limitations of existing approaches we propose a novel scheme, by which the quality of their covered true image is maintained. Moreover, this scheme does not involve use of keys for encryption of images, has low storage and bandwidth requirements, while also keeping less computation cost during encryption and decryption.

Security of data and image has grown and evolved significantly in recent years. To Maintain the secrecy and confidentiality of images is two different approaches are being used, the first encrypting the images through encryption algorithms using keys, the second approach involves dividing the image into random no of shares to maintain the images secrecy. But it has also the problem of poor quality of the recovered image. So a novel approach without encryption key is proposed in this paper. One of the main objectives of the proposed system is to maintain the secrecy and confidentiality of data and images. The major steps involved in this approach arefiltering also called Sieving, Division and Shuffling to generate random shares such that with less computation, the true secret image can be recovered from the random shares without any loss of image quality. The total numbers of shares needed by the authenticated entity and number of the shares being given to the receivers or clients are generated using random number generation algorithm.

Data encryption can also be done by converting the data into an image. This project will provide a system to serve both sender and receiver of the secret message. To provide more security to the data, authenticated entity will keep the fingerprint of the original receiver. After the fingerprint authentication, the secret image is transmitted to the

authenticated entity. This transmission can be done in the wireless sensor network by any data transmission technique like Kerberos data transmission technique, email etc.

In this paper section 2 discuss about the related works. Section 3 describes about how to secure images by SDS approach for secrecy. Section 4 presents the algorithm of this proposed system. Section 5 illustrates the experimental result of the algorithm. Finally section 6 concludes the paper with the highlights.

RELATED WORKS

Image Encryption:

There are lots of schemes arises in the last few decades for image encryption using keys, some of the prominent ones have been here. Manniccam and Bourbakisin 1992 proposedan image encryption and compression scheme using SCAN [4]languageis the main. The scheme was typically based on chaos theory. But this was applicable to only grey scale images. LikewiseXin and Chen [2] in 2008 following up on the work of proposed a two stage image encryption scheme. Fusion of the original image and the key image involved in the first step and step two involved encryption of the fused image using Henon chaotic system [10]. Chen, Hwang and Chen in 2000 proposed the Vector Quantization (VQ) technique for designing a cryptosystem for images. After all traditional cryptosystems are used.

Visual Cryptography:

The idea of Image splitting more often described as Visual Cryptography Schemes (VCS) [5] involves splitting a secret image into n random shares in such a way that these shares individually convey no information about the secret image but an eligible subset of the shares; specified by the encrypter when stacked up convey the secret image. The random image shares of eligibleset are merely printed on transparencies and stacked up uncover the original image. The major problems which restrict its employment is the poor quality of the recovered image, limited colour representation etc. Many research papers has been published using this approach, starting from a binary image coming to grey scale image and finally employing it to colour images. Although with each subsequent research paper the quality of the recovered image improved, however, but for no other scheme was able to completely

recover the original image from the shares that are retrieved. When evaluating the performances of these suggested solutions they are often on performance measures such as contrast, accuracy, computational complexity etc. and more for security. Thus an ideal solution would recreate the original image from the shares in terms of colours and contrast; it would also have to be secure and computationally inexpensive.

In Hybrid approach image is split into random sharesusing some kind of an encryption key. Incze et al proposed [12] the concept of sieves for encryption of images. Sieve is basically a binary key. The original image is placed above the sieve. Pixels from the original image placed above a hole of the sieve go through and form one share of the image. The pixels that remain on the sieve on a black pixel will form the other share of the image. From the analysis of the various cryptographic approaches for images, it is appreciated that the essentials for any cryptographic scheme would involve low computation cost, retrieval of original image, absence of keys and robustness to withstand.

The transmission of shares can be done in the wireless sensor network by any data transmission technique like Kerberos data transmission technique, email etc. Kerberos [1]uses the symmetric Needham-Schroeder protocol. It makes use of a trusted third party, called a key distribution centre (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS) to control the functions. The KDC maintains a database of secret keys; each entity on the network — whether a client or a server — shares a secret key known only to itself and to the KDC only. Knowledge of this key helps to prove an entity's identity. For communication purposes the KDC generates a session key which communicating parties use to encrypt transmissions between them. The security of the protocol relies completely on short-lived assertions of authenticity called Kerberos ticket.

PROPOSED SCHEME

As shown in Fig 1 the proposed method involves two steps i.e. image encryption and second step is the transmission of the secure image only to the authenticated receiver. Receiver authentication is achieved by using fingerprint comparison. We are using this authentication step as a second security level even though the encrypted image reveal no

information about the original image. The shares will be delivered to the receiver only if he or she is an authenticated entity.

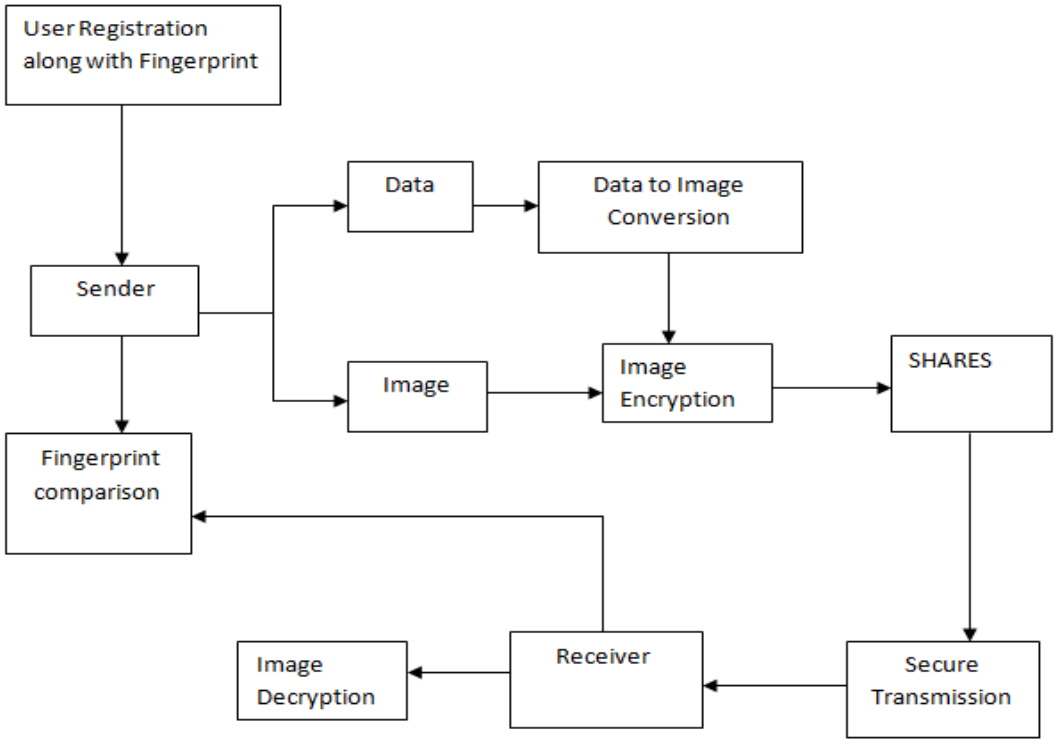

Fig 1. Proposed method

Data encryption can also be done using the same encryption technique. Here the data will be converted to image and undergoes the same steps as of image encryption. And one main advantage is that the user can enter data in their own language. This data to image conversion is completely hidden from the user. So we can say that the system is more users friendly.

The steps included in encryption techniques are:

1) Seiving:

Sieving is the process of filtering the combined RGB components into individual red, green and blue components. The the state or quality of the sieve being grainy depends the

range of values that R/G/B component may take individually. Seiving is done using XOR operator to reduce the cost of computation.

2)Division:

After filtering the real image into the red, green and blue components, the second step includes dividing the Red, Green and Blue components into no of required shares each. This no shares required is determined by the random no generation algorithm. Consider the no of shares required is 3. Then the red, green and blue images split into 3 shares according to the encryption algorithm.

Red Shares - (RA, RB, RC)

Green Shares - (GA, GB, GC)

Blue Shares - (BA, BB, BC)

During division it is ensured that each element in RA-C, GA-C and BA-C is assigned values in random order, such that the entire domain is available for randomized selection; in case x = 8, then individual elementswould be randomly allocated a value varying from 0-255. The shares so generated should be in such a way that (RA, RB, RC) should regenerate Red, green and blue components.

3)Shuffling:

Although the experimental results have shown that the output created by division processdoes not have any resemblance to the original image, but as a second security step towards randomizing the created shares i.e. RA-C, GA-C and BA-C , we perform the shuffle operation. This involves shuffling the pixel values in the individual red, green and blue shares. The sequence in which the pixel values within the shares are shuffled depends on the value of one of the other shares generated from the same primary colour. In other words RB decides how RA is shuffled; RC decides how RB is shuffled etc. The shuffling operation is done using comparison operator.

4)Combine:

At the end of these three main steps, the final share is obtained by combining corresponding shares as follows:

Random share A - (RA- shuffle, GA- shuffle and BA- shuffle)

Random share B - (RB- shuffle, GB- shuffle and BB- shuffle)

Random share C - (RC- shuffle GC- shuffle and BC- shuffle)

ALGORITHM

Input: Plain image, Data

Output: Encrypted Image

Step 1: Convert data to image if the inputis data. Else move to step 2 directly.

Step 2: Seiving

Step 3: Division

n = total number of pixels i.e. 0 to n-1.

Ri / Gi / Bi = individual values of the i'thpixelvalue in the R, G, B components.

S = total no of random shares

x =number of bits representing each pixel

maxval = 2x

Repeat 2 for R, G, B component

for i = 0 to (n-2)

{

for share k = A to (S-1)

Rki = Random (0, maxval)

AggrSumi= Rki

}

Rzi=(maxval + Ri – (AggrSumi % max_val)) % maxval

```
for k = A to S
 {
        Rk-shuffle = Rk
        PtrFirst = 1
        PtrLast = n-1
        For i = 1 to (n-1)
        {
        If (R(k+1)(i-1) is even)
        {
        R(k-shuffle) PtrFirst= Rki
                PtrFirst ++, i++
        }
        Else
        {
                R(A-shuffle)
                PtrFirst = RAi
        i++;
                PtrLast --
        }
        }
}
```

Step 4: Shuffle

Repeat for all generated shares

Step 6: Combine

For k = A to S

Random Share k = Rk-shuffle XOR Gk-shuffle XOR Bk-shuffle

At the end of all these above processes we have Random shares (RSA ,RSB --).

Step 7: Transmission of encrypted shares using any transmission technique to the Authenticatedreceiver. Authentication of the receiver isdone using fingerprint technology.

EXPERIMENTAL RESULT

Experiments were carried out on various images using this proposed algorithm. The testedimagesareretrieved in totality.Toprove the accuracy of our algorithm we implemented a modified (2, 2) threshold visual cryptographic scheme. This scheme was identified to provetheresults as this could have it are real world application to authenticate a user. A photograph of an authenticated could be clicked and divided into two shares. One of the shares would be held by the authenticating agency and the other would be held by the user who is being authenticated. It can also use in group business where there is no trust among them. The process of creating two random shares has been explained below.We implemented the scheme on the NetBeans platform using java. The scheme was run over a wide range of photographs including coloured, black and white etc. Consider a 300 X 168 pixel image with an image depth of 24 bits i.e.8 bits each for Red, green and blue pixel value. The various parameters as defined in the generic algorithm above thus take the following values.

n = (300 * 168) = 50400 i.e. n varies from 0 to
50399
k = total random shares = 2 i.e. Share A, share B
maxval = 2^x
= 2^8
= 256, x = 8
PtrLast= (n-1) = 50399

The process of retrieving the original image includes 4 steps; that are the reverse of steps included in encryption. First step is un-combining afterobtainingthe 2 encrypted shares.Then these un-combined shares are un-shuffled each within itself to get the original

image. Later, the un-shuffled image is split into primary colours. After merging these primary colours, we will get the original secret image without any loss of image quality.

CONCLUSIONS

In this paper a novel visual cryptographic technique is presented, which is a combination of the traditional visual cryptographic scheme and the conventional image encryption schemes. A secret image is divided into multiple random shares and with minimum computational cost the true secret image can be retrieved back. The proposed algorithm has the following advantages (a) The original secret image can be retrieved without any loss in colour and contrast (b) There is no pixel expansion problem and there by storage requirement per random share is same as original image (c) No key management problem since we are not using any keys for encryption (d) The system is robust to withstand brute force attacks with lower cost.

REFERENCES

[1] Subramanian Kalyan, R.Vignesh, UjjvalH.Thakkar, T.Adiline Macriga4 3rd Year, Department of of Information Technology, Sri Sairam Engineering College Chennai, India."*MISTIKOS-on Communication Secure Data Transmission In Wireless Network* "2012 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[2] Xin Zhang and Weibin Chen, "*A new chaotic algorithm for image encryption*", International Conference on Audio, Language and Image Processing, 2008. (ICALIP 2008), pp 889-892.

[3] AlokaSinha and Kehar Singh, "A technique for image encryption using digital signature", Optics Communications(2003),218(4-6),pp229-234.

[4] S.S.Maniccam, N.G. Bourbakis, "Lossless *image compression and encryption using SCAN*", Pattern Recognition 34 (2001), pp 1229-1245.

[5] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "*A new encryption algorithm for image cryptosystems*", The Journal of Systems and Software 58 (2001), pp. 83-91.

[6] A. Shamir,"*How to share a secret*," *Commun.ACM*, vol. 22, no. 11, pp.612–613, 1979.

[7] M. Naor and A. Shamir,"*Visual cryptography*," in *Proc. EUROCRYPT'94*, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[8] C.C Chang, T.X Yu, "*Sharing a secret gray image in multiple images*", in:Proceedings of First International Symposium on Cyber Worlds,2002,pp.230-240.

[9] H.-C. Wu, C.-C. Chang, "*Sharing Visual Multi-Secrets Using CircleShares*", Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).

[10] Hanan Mahmoud HananSaad Al-Hulaibah Sarah Ahmad Al-Naeem,"*Novel Technique for Steganography in Fingerprints Images: Design and Implementation*",Department of Information Technology, College of Computer and Information Sciences, Centre of Excellence in Information Assurance King Saud University, Kingdom of Saudi Arabia.

[11] Wikipedia: http://en.wikipedia.org/wiki/Encryption.

[12] Arpad Incze, "*Pixel sieve method for secret sharing &visualcryptography*" RoEduNet International Conference Proceeding Sibiu24-26 June 2010, ISSN 2068-1038, p. 89-96.