ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 10, October 2017

PERFORMANCE EVALUATION FOR SECRET SHARING IMAGE USING SHAMIR VISUAL CRYPTOGRAPHY IN CLOUD APPROACH

Mamta, Mrs.Niyati Jain

[#]*M.Tech Computer Science, MDU,Vaish College of Engineering*
Rohtak, Haryana
mamtachugh84@gmail.com
jainniyatiojas@gmail.com

ABSTRACT

Cloud Computing offers enormous benefits to its adopters, but it also comes with its set of problems and inefficiencies of which security is the biggest concern. Secret sharing refers to a process of distributing a secret among a group of participants, where each participant is issued with a share of the secret. The secret can be reconstructed by combining the participants' shares. Single individual participants share is of no use. This paper proposes a (p,n) secret sharing approach for secret images using Shamir visual cryptography model. The secret image pixels and the participant's numerical key are used in the reversible polynomial function to generate 'p' secret shares. The sender distributes the generated secret shares to 'P' participants' .During reconstruction the RGB color channel process is used to reconstruct the secret image. The secret is reconstructed by combining 'n' secret shares. The secret is reconstructed without loss.

Keywords: Secret image sharing, cryptography, information security visual quality of image, pixel expansion etc.

I. INTRODUCTION

We start our description of security in distributed systems by taking a look at some general security issues. First, it is necessary to define what a secure system is. We distinguish security policies from security mechanisms, and take a look at the Globes wide-area system for which a security policy has been explicitly formulated. Our second concern is to consider some general design issues for secure systems. Finally, we briefly discuss some cryptographic algorithms, which play a key role in the design of security protocols. Security in computer systems is strongly related to the notion of dependability. Informally, a dependable computer system is one that we justifiably trust to deliver its services. Dependability includes availability, reliability, safety, and maintainability. However, if we are to put our trust in a computer system, then confidentiality and integrity should also be taken into account. Confidentiality refers to the property of a computer system whereby its information is disclosed only to authorize parties. Integrity is the characteristic that alterations to systems assets can be made only in an authorized way. In other words, improper alterations in a secure computer system should be detectable and recoverable.

Major assets of any computer system are its hardware, software, and data. Important security mechanisms are:

1. Encryption
2. Authentication
3. Authorization
4. Auditing

Encryption is fundamental to computer security. Encryption transforms data into some- thing an attacker cannot understand. In other words, encryption provides a means to implement confidentiality. In addition, encryption allows us to check whether data have been modified. It thus also provides support for integrity checks. Computing is a computing paradigm, where large pools of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and _le storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities.

II. SECRET SHARING

Secret sharing was first proposed by Shamir and independently by Blakley. These seminal schemes operate under a very simple model: a trusted dealer

has a secret and distributes a different share of that secret to each server. Shamir demonstrates that a passive adversary who learns up to t shares of the secret gains no partial information about the secret, yet any t + 1 servers can combine their shares to recover the secret. Blakley's scheme makes a similar guarantee, except that it does not provide perfect secrecy; combinations of t or fewer shares reveal partial information about the secret, and additional modifications are needed to ensure perfect secrecy. Shamir's scheme is based on interpolation of polynomials over a finite field, whereas Blakley's scheme encodes the secret as an intersection of ndimensional hyper planes. Each share in Shamir's scheme is the same size as the original secret, but shares in Blakley's scheme are t times as large. Shamir's scheme is more widely used because it provides stronger guarantees and better space efficiency using only relatively simple mathematics. The PSS scheme of Zhou et al. is based on a different secret sharing mechanism that is even simpler but more limited than both Shamir's and Blakley's schemes.

III. DISTRIBUTED CLOUD COMPUTING

Recent research in the area of distributed cloud computing has given capable new directions to threshold cryptography in the field of cloud computing, which has set off a transforming change in the traditional ways of computing. As almost all of the previous standalone software, ranging from file managers to office automation tools, have taken their incarnations in the cloud, the user base of cloud-based tools and services has inflated to a huge extent. This usage shift to cloud technology has put forward new challenges to computer scientists. Cloud computing involves storing users' private data at a remote location. This breaks the implicit security of personal devices, and researchers have come up with innovative solutions to address the security concerns so as to ensure confidentiality, integrity, and access control.

IV. PROBLEM STATEMENT

As security is sensitive issue in cloud computing .the data are coming from cloud using public network (internet) there are chances to hack the data. Here a lot of work done on safety issues and issues but still here is not 100% full proof solution. There are many physical and some other attack on data that destroy data on server. one clarification for that is distributed the information on more than one server in its place of one server .but this not solve problem completely because data stored in encrypted mode using encryption key .the attackers attack on key and may be hack the data.

V. PROBLEM SOLUTION

Hackers attack on secure data which is placed on same server. So that solution is doing multiple copies of similar data and data is placed on multiple servers. But data is encoded by encrypted key. Hackers may be attack on key so that information is exposed to the attackers. The solution of this problem is instead of situating multiple copies of data on different server we are relating Shamir‟s secret sharing on key. The encoded key is distributed into no. of fragments and stored them on different server. But again if attackers attack on one of the server that slice of the key is misplaced but still it can rebuild the key using Shamir‟s threshold order which uses threshold value it is useful on the key. The most famous perfect secret sharing scheme is the (k, n)-threshold system first recommended through Shamir in 1979 and here mentioned to as a Shamir threshold system. A key can be reassembled again with minimum number of secret which are on different server there is no difficulty if Hackers attack on one server. The reaming server can rebuild key. This secret Shamir‟s system reduce the problem of key conversation .Shamir‟s scheme uses lag ranges of polynomial to divide the key in number of pieces Secret sharing refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be rebuilt one when an appropriate no. of shares is joined composed; individual shares are of no use on their own. More formally, in a secret sharing scheme there are one dealer and n players. The sender provides a secret to the receiver, but only when precise circumstances are satisfied. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no collection of less than t receiver can. Such a system is called a (k, n)-threshold scheme (sometimes it is written as an (k-n) threshold scheme).

VI. SYSTEM MODEL

Shamir's Secret Sharing

Shamir‟s calculation is executed in view of the protected request safeguarding method talked about in Shamir‟s calculation is connected to each field of the table. The n shares got are then conveyed to various server farms out of which just k of the offers

are required to accomplish the first esteems. It is conceivable to bolster organized questioning of the information parsing the inquiry, extricating the contingent esteems, changing the qualities and attaching them back to the first question before it is sent to the server. Converse of Shamir"s Secret sharing calculation must be connected to the gotten informational collection to get back the proposed result. Accept that the table „employees (emp_no, compensation, empname)" is outsourced. The customer ought to have the capacity to execute the accompanying kind of questions without uncovering the information to any of the Database specialist organizations.

A. Principle

The basic idea behind secret sharing algorithm is, when we want to secure a certain data _D', we divide it into n parts say D1, D2…,Dn in such a way that:

• The Knowledge of any k or few Di pieces makes D easily computable.

• The Knowledge of any k-1 or fewer Di pieces leaves D completely undetermined (in the sense that all its possible values are equally likely). This scheme is called (k,n) threshold scheme. The value of factor K can be decided depending on the level of security we desire. For example, if the data is of top most priority such as bank account password or transaction ids we can keep k=n. In such a case all participants will be required to reconstruct the secret original data.

B. Mathematical Operation

The mathematical implementation of Secret Sharing algorithm can be understood with the help of a simple example as given by MdKausar et al. in [11]. The generalized idea is as follow:

• We choose at random (k-1) coefficients i.e. a1…a_{k-1}

• We divide our secret data 'S' by picking a random degree polynomial

$q(x) = a_0+a_1x+a_2x^2 +\ldots+a_{k-1}x^{k-1}$
Where a_0= 'S' (i.e the data).

Now if we wish to divide the data into n parts, we will substitute 'n' different values of x in the polynomial q(x) and obtain _n' such sets of (x, y), here y is nothing but our polynomial q(x).
The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes "k" points to define a polynomial of degree "k-1". Select 'k' such sets, any k combination of the available n parts will generate the same result. The value in these sets are meaningless alone, it is only when 'k' sets are brought in together and further worked upon that we get our secret back. These "k" instances of original polynomial are processed using Lagrange polynomials. The Lagrange basis is:

$$l_0 = \frac{x - x_1}{x_0 - x_1}\cdot\frac{x - x_2}{x_0 - x_2}$$

$$l_1 = \frac{x - x_0}{x_1 - x_0}\cdot\frac{x - x_2}{x_1 - x_2}$$

$$l_2 = \frac{x - x_0}{x_2 - x_0}\cdot\frac{x - x_1}{x_2 - x_1}$$

Substitute the values of x from the selected _k' sets into the Lagrange basis and we obtain _k' fractional equations for the same. Finally on taking summation of the equations obtained from Lagrange basis and y form the selected _k' sets, we get back our original polynomial. The summation can be represented mathematically as:

$$f(x)=\sum_{j=0}^{2} y_j.l_{j(x)}$$

The above explanation helps in understanding the working of the secret sharing algorithm. When done manually the entire calculation can be done in minutes, while on implementation, as the microprocessor technology has elevated its level to a new high, thousands of such calculations can be done in seconds.

C. Properties

The secret sharing algorithm possesses some dynamic properties that make it further more powerful, these properties, as descried by Adishamir in [4] are as follows:

• The size of each piece does not exceed the size of the original data.

• When k is kept fixed, D pieces can be dynamically added or deleted without affecting the other Di pieces.

• It is easy to change the Di pieces without changing the original data D - all we need is a new polynomial q(x) with the same free term. This can enhance security.

• By using tuples of polynomial values as Di pieces, we can get a hierarchical scheme in which the number of pieces needed to determine D depends on their importance.

VII. PROPOSED METHOD

Recently, the transmission of data through network is increasing rapidly, which provides instant access or distribution of digital data. Visual cryptography is the technique using in the latest technology to transmit the secret information in images i.e., called secret image. Secret data sharing is the significant substance in the field of communication tools, information security and production. However security can be introduced in many ways like transmitting password, image hiding, watermarking technique, authentication and identification. But the drawback of these methods is that the secret images can be protected in single information carrier. If it lost once, the information carrier is either damaged or destroyed. To overcome this problem, VCS secret sharing scheme was introduced by Naor and shamir[1], the secret image is split up into number of shares and transmit to the number of participants. A visual secret sharing system is a method used to encode the secret image by unbearable the shares into numerous piece and allocate it into the consistent participants. A set of qualified participants can be able to retrieve the secret image by overlapping the shares in correct order. A outmoded VCS proceeds the secret image as input and no. of shares as output, it fulfills two circumstances 1) secret images can be recover by any qualified subset of any forbidden subset of shares cannot gain any information about the secret image. For example, In traditional (k,n)-VCS, the secret image is revealed if k of n shares are known. Any number of n shares less than k is not sufficient to reveal secret image where, k is the number of participants and n is the number of shares.

In general, three main processes are implemented in this system. At the sender side, the preprocessed secret image can be encrypted by using the GAS (General Access Structures) solver algorithm. This image can be protected by using the password authentication. The share synthesizer splits the image into the number of shares as per the number of participants can be done in the generate shares phase. By the side of the embedding stage, the shares can be marked with the cover images. The embedded images are now ready to send it to the receiver. At the receiver side, the shares can be mined from the cover images. Thus by overlapping the shares in an order with the correct password verification, the secret image can be retrieved at the extraction phase.

Visual cryptography

The (2, 2) VC System [2] use to encrypt the secret, the new image is divided into two Shares such that, unique image pixels is substituted with non-overlapping block of two sub-pixels. A white pixel is shared into two equivalent blocks of sub-pixels. A black pixel common into two consistent blocks of sub-pixels. For the decrypting of image, loading both the shares will permit the visual retrieval of the secret. While making the shares, if the pixel pin the unique image is white, then the encoder arbitrarily selects the first two columns of fig 1.

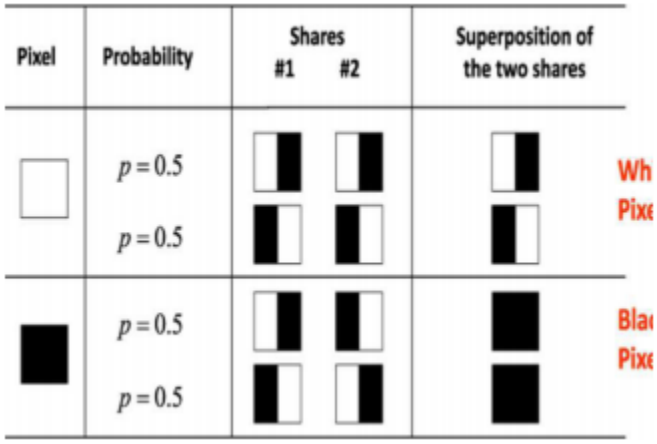

Figure : 1 display 2-out-of-2 VCS system with 2 sub-pixel construction

In (2, 2) VCS, every pixel P in the original image is encoded into two sub pixels called shares. Fig.1 signifies the shares of a black and a white pixel. The excellent of shares for a white and black pixel is casually resolute. Neither share gives specific proposal around the novel pixel since dissimilar pixels in the secret image will be encoded using independent random choices. When stack the two shares, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if P is a white pixel, we get one black sub pixel and one white sub- pixel.

The proposed scheme consider security of image in terms of encrypting it with the help of symmetric key, hence if someone access all the shares in unauthorized way, he/she cann‟t decrypt it completely without symmetric key. This scheme

manages security as well as decrypted images are of same size as original. The scheme is divided into three parts: Encryption of original image using symmetric key.

Generation of Shares

Decryption of Overlapped shares

Encryption Process

Distribute images into blocks such that block size equivalents to key size.

Each block is XORed with key and then placed again in its original position.

Currently, encrypted image is separated into shares using visual cryptology.

Share Generation

To overcome the increasing size problem, following approach is used for share generation. By considering 4 pixel of input image at a time and then generating 4 output pixels for each share.

There are 16 cases which are in following 5 Categories.

Shares and symmetric key is transferred to the receiver. We can also divide the symmetric key into shares for more security.

Decryption Process

At Receiver site, shares are combined and combined share is divided into blocks such that block size equals to key size. Each block is XORed with key and then placed again in its original position. Now original secret image is recovered.

VIII. SIMULATION RESULT

Simulation results for the proposed secret sharing scheme for color images are illustrated in this section. The experiment was conducted for different color images of size 512 x 512. The embedded secret image is of same size as the original image.

At the sender side, the input secret image generates shares based on visual algorithm which done in the first phase. At the receiver side, the embedded images can be processed to extract the covering images from the generated shares and the secret images can be retrieved by overlapping the shares in the correct order.

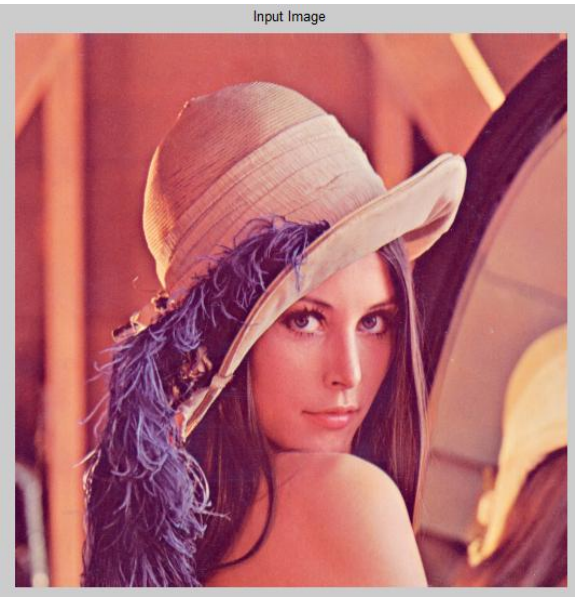

Figure 2: Input image for simulation

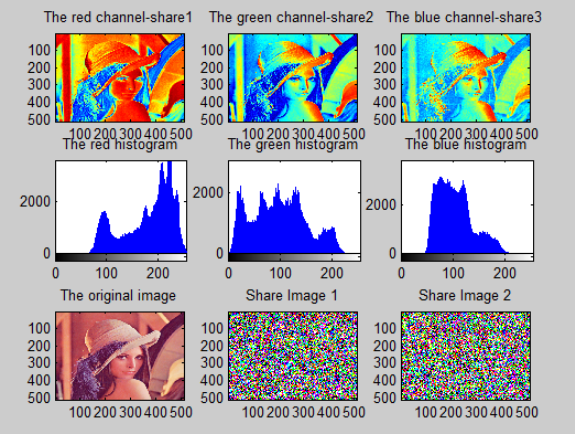

Figure 3: RGB channel with histogram and share 1 and share 2

RGB channel shows the image is 24-bit (the industry standard as of 2005), each channel has 8 bits, for red, green, and blue—in other words, the image is composed of three images (one for each channel), where each image can store discrete pixels with conventional brightness intensities between 0 and 255.

Figure 4: The output image with superimposed in VC

Extract the embedded cover images and secret shares. By stacking the shares in the correct order will get an original secret image with share 1 and share 2 is done using the proposed algorithm. At the receiver side it stacks the shares by using the logical or operation and extracts an original secret image. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image

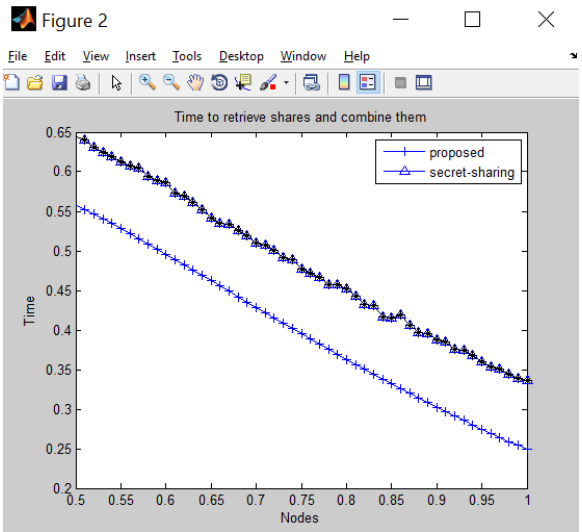

Figure 5: Accuracy graph as time to retrieve

In this figure curve shows the accuracy parameter and black point shows the fitted value in this curve. It presents how much time taken to fit data in proposed line.

IX. CONCLUSION

Visual cryptography exploits the security to decrypt the secret image with no computation required. As we are divide the input into multiple visual encrypted in three parts like RGB. The pixel expansions and contrasts derived from our HVCS are better than the previous results. The contrasts of different secret regions can also be designated in the constraints. This enhances the adaptability and flexibility of our HVCS in practical applications. The given input image can be divided into secret sharing parts which can be used in future for Encryption. We would be using genetic algorithm for implementation of this Encryption technique. Paper suggests VSS, but we would be developing as it is a better and more robust algorithm for image encryption. This paper exploits the techniques of Halftone technology. The proposed scheme revealed good security due its randomness.

REFERANCES

[1] L. Bai. A reliable (k,n) image secret sharing scheme. In DASC.pages 31–36. 2006

[2] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbooks of Applied Cryptography.CRC Press. ISBN: 0-8493-8523-7. 816 Pages. 1996

[3] C. Huang and C. Li. Secret Image Sharing Using Multiwavelet Transform. Journal of Information Science and Engineering, 733-748. 2011.

[4] JagdeepVerma, danVineetaKhemchandani. A Visual Cryptographic Technique to Secure Image Shares, International Journal of Engineering Research and Applications (IJERA), ISSN : 2248-9622, Vol. 2, Issue 1, pp.1121-1125. 2012

[5] Widyadhana, Arya, danMuchmamadHusni. Penerapan Secret Image Sharing MenggunakanSteganografidenganMetode Dynamic Embedding dan Authentication-Chaining, JurnalTeknik ITS, Vol.1. ISSN: 2301 – 9271. 2012

[6]. Ion Morozan, "Multi-Clouds Database: A New Model to Provide Security in Cloud Computing". 2012

[7]. D.Mounica, Mrs.Ch.Radhika Rani "Optimized Multi-Clouds using Shamir Shares" International Journal For Development Of Computer Science & Technology ISSN-2320-7884 ,VOLUME-1, ISSUE-III, Hore et al. (April-May 2013) .

[8]. MdKausarAlam, SharmilaBanu K. "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds". International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153.

[9]. PriyankaPareek, "Cloud Computing Security from Single to Multi-clouds using Secret Sharing Algorithm". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12, December 2013.

[10]. Sonia Verma1 and Amit Kumar Chaudhary, "Save And Secured Data On Clouds" Volume 5, No. 4, April 2014, Journal of Global Research in Computer Science.

[11] MdKausarAlam, SharmilaBanu K, ―An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds,‖ International Journal of Scientific and Research Publications, vol. 3, issue 4, April 2013