INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ENGINEERING RESEARCH AND DEVELOPMENT (IJCSERD)

ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online),
Volume 4, Number 2, April- June (2014), pp: 1-8

IJCSERD

© PRJ PUBLICATION

KEYLESS APPROACH OF SEPARABLE HIDING DATA INTO ENCRYPTED IMAGE

[1]Sameenah S B, [2] Mrs. Vandana B S

[1]Department of Computer Science and Engineering, KVGCE, Sullia, DK VTU Belgaum
[2]Asst. Professor, Department of computer Science and engineering, KVGCE, Sullia, DK, VTU Belgaum,

ABSTRACT

The heavy computation cost and the poor quality of the recovered image from the random shares restrict the applications, by the use of encryption keys. Key management is difficult dispute in network. This paper presents a unique method of data hiding separately in an encrypted image. This work presents a new method that combines image cryptography, data hiding and LSB compressing technique for data hiding separately. Then, a data-hider compresses the least significant bits of the encrypted image to create a sparse space to accommodate some additional data. This paper proposes without the use of keys, encrypting and decryption of image and data is done. In this method we encrypt the original image with SDS algorithm. The approach employs Sieving, Division and Shuffling to generate random shares. Then cover the encrypted image by a grayscale image such that with a minimal computation the original secret image can be recovered from the random shares without any loss of image quality.

Keywords: Data embedding, Sieving, Division, Shuffling, Random shares.

I. INTRODUCTION

Encryption is a process of converting messages, information or data into a form unreadable by anyone except the intended recipient [1]. Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. The root of the word encryption crypt comes from the Greek word crypto's meaning hidden or secret. In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures, in chronology the history of Cryptography [2] throughout centuries. For different reason humans have been

interested in protecting their messages. The Assyrians were interested in protecting their trade secret of manufacturing of the pottery. The Chinese were interested in protecting their trade secret of manufacturing silk. Cryptanalysis is the art of breaking cryptosystems. Cryptology is the study of both cryptography and cryptanalysis. Today's cryptosystems are divided into two categories: symmetric and asymmetric. Symmetric crypto systems use the same key [3] (the secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key(the private key) to decrypt it by some algorithms.

Encryption has been used by people in all situations such as in corporate, military and personal information. Encryption is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In this method, the message or information referred to as plaintext and image is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a key which adversaries do not have access to. There are two basic types of encryption schemes: Symmetric-key and public-key. In symmetric-key schemes, the encryption and decryption keys are the same. Thus communicating parties must agree on a secret key before they wish to communicate. In public-key schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages. Public-key encryption is a relatively recent invention: historically, all encryption schemes have been symmetric-key [4] also called private-key schemes. Encryption is also used to protect data in transit, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message. Digital signature and encryption must be applied at message creation time Otherwise any node between the sender and the encryption agent could the encryption device itself has not been tampered with. Other approach adopted for maintaining confidentiality of images is image splitting involves splitting an image at the pixel level into multiple shares i.e. two or more, such that individually the shares convey no information about the image, but a qualified set of these shares will help regenerate the original image at least partially. It is also referred as Visual Cryptography Schemes (VCS) [5] involves splitting a secret image into n random shares such that these shares individually reveal no information about the secret image but a qualified subset of the shares when stacked up reveal the secret image. The random image shares are merely printed on transparencies and stacked up revealing the original image.

Data Hiding [6] is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data(Image). The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication, however the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out.

II. RELATED WORK

A number of data hiding method have been proposed in recent years. In difference expansion method [1], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. The KUDOS cryptographic algorithm basically falls under the symmetric encryption i.e. the same key is used at both ends to encrypt and decrypt the data. However, KUDOS actually depends on the sequence counter instead of the encryption key. A. Sinha and K. Singh [6] have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is embedded to the encoded version of the original image prior to detect an error control code such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image. This encryption technique provides three layers of security [7]. In the first step, an error control code is used which is determined in real-time, based on the size of the input image. Without the knowledge of the specific error control code, it is very difficult to obtain the original image. Many research papers have been published using this approach, starting from a binary image [7, 8] moving to greyscale image and finally employing it to colour images. Though 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.

Many research papers have been published using this approach, starting from a binary image moving to greyscale image [9] and finally employing it to colour images. Though 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.

Encryption of images with the traditional encryption algorithms such as RSA, DES etc. was found inapt due to some typicality's of images such as its bulk size as also the correlation amongst the pixels. This gave rise to a new area of research for encrypting images.es. This approach is basically similar to the conventional encryption methods which involved using an algorithm (and a key) to encrypt an image. Some of the proposed techniques for encrypting images use "Digital Signatures" , "Chaos Theory" , "Vector Quantization" etc. to name a few. There are some inherent limitations with these techniques; they involve use of secret keys and thus have all the limitations as regards key management. In addition, in some cases the available keys for encryption are limited (restricted key space). Also high computation involved in encryption as also weak security functions are also an issue [9]. However the greatest strength Adi Shamir in 1979 is credited for introducing the idea of dividing a secret data into 2 random shares. In 1995, Naor and Shamir, using this as the basis, proposed the concept of "Visual Cryptography", which involves secret sharing of an image by dividing it into multiple shares. Many variations to the scheme proposed in have been researched to overcome its limitations, each having their own merits and demerits. Last few decades have seen lots of schemes being proposed for image encryption using keys, some of the prominent ones have been here. Manniccam and Bourbakis [10] in 1992 proposed an image encryption and compression scheme using SCAN language. The scheme was fundamentally based on chaos theory. However this was applicable to only grey scale images. Similarly Xin and Chen [10] in 2008 following up on the work of, proposed a two stage image encryption scheme. Step one involved fusion of the original image and the key image and step two involved encryption of the fused image using Henon chaotic system.

III. PROPOSED SYSTEM

This paper proposes a simple and effective method to encryption of image where data embedded into encrypted image at sender side then decryption is takes place at receiver side to extract image and data separately. The Encryption and Decryption Model is as shown in Fig1:

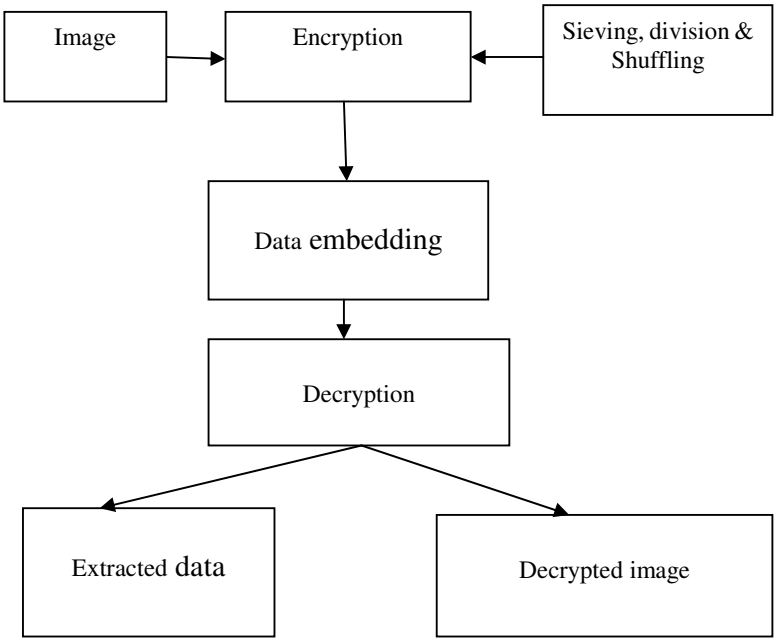

Fig. 1. Encryption and Decryption model

A. Data Embedding

In Data embedding, data hiding is done by the data hider. Pseudo-random permutation of pixel is done in order to reduce the intelligible information .LSB of encrypted pixels are compressed to create a space for accommodating the additional data and the original data .the detailed steps are as follows. The Steps for Data Embedding is as follows:

1. Data hider first selects the data.
2. Some parameters for data hiding are embedded in small number of encrypted pixels.
3. Remaining encrypted pixels are pseudo-randomly permuted and divided into number of groups of X pixels.

B. Encryption and Decryption Proposed algorithm

The algorithm is mainly divided into three steps they are: sieving, dividing and, shuffling as shown in Fig 2. The sieving involves the secret image splitting into primary colors. The second important step is division, which involves the random division of the split image. In the third step, the divided Shares are shuffled randomly.

Step 1:
Input the secret image. Sieve is applied for input image then the output for the input image will be based on the primary colors.
Sieve (input image)
Output will be the R, G, B components.
Step 2:
Division is based on the number of pixels.
Let n be the total number of pixels
(0 to n-1)
Let Ri Gi Bi is the individual values of the pixel in the R G B components.
Total number of shares is Z
Total number of bits representing the primary colors is x.
MAX_VAL=2^X
Step 3:
Shuffle R (A-Z) G (A-Z) B (A-Z) for all shares.
Step 4:
Combine A to Z of R, G and B colors by $R_{SHUFFLE}$ XOR $G_{SHUFFLE}$ XOR $B_{SHUFFLE}$ for decryption.

C. Modules

The modules of SDS algorithm for image encryption are as follows:

- Sieving.
- Division.
- Shuffling.

1) Sieving

Sieving as the name suggests involves filtering the combined RGB components into individual R, G and B Components [11]. To make the process computationally inexpensive, sieving use the XOR operator. The modular diagram for sieving is shown in Table 1 as follows:

R	G	B
R	0	0
0	G	0
0	0	B

Table 1. Sieving modular diagram

2) Division

Having filtered the original image into the R, G and B components, the next step involves dividing the R, G and B components into z parts/ shares each is as follows,
R = (RA, RB, RC, ----------, RZ)..... (I)
G = (GA, GB, GC, ----------, GZ)..... (2)
B = (BA, BB, BC, ----------, BZ)..... (3)

While dividing it is ensured that each element in RA-Z, GA-Z and BA-Z is assigned values randomly, such that the entire domain is available for randomized selection; in case x = 8,then individual elements should be randomly assigned a value varying from 0- 255[11]. The

shares so generated should be such that (RA, RB, RC, ---------- RZ) should regenerate R and similarly for G/B components.

3) Shuffling

The random shares created by division in no way exhibit any resemblance to the original image, but as a second step towards randomizing the generated shares i.e. RA-Z, GA-Z and BA-Z, we perform the shuffle operation [11]. This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary colors. In other words RB decides how RA is shuffled, RC decides how RB is shuffled, ---------- RZ decides RZ-1 is shuffled and RA decides how RZ is shuffled. The Shuffling operation uses the comparison operator on the LSB of the determining element to decide the shuffle sequence. Having carried out the above three operations the generated shares are combined to generate the final z random shares (RS) is as follows,

RSA = (RA- shuffle, GA- shuffle and BA- shuffle)

RSB = (RB- shuffle, GB- shuffle and BB- shuffle)

- -- - - -
- - - - - -
- -- - - -
- -- - - -
- -- - - -
- -- - - -

RSZ = (RZ- shuffle GZ- shuffle and BZ- shuffle).

The division and shuffling modular diagram is shown in Fig 3:

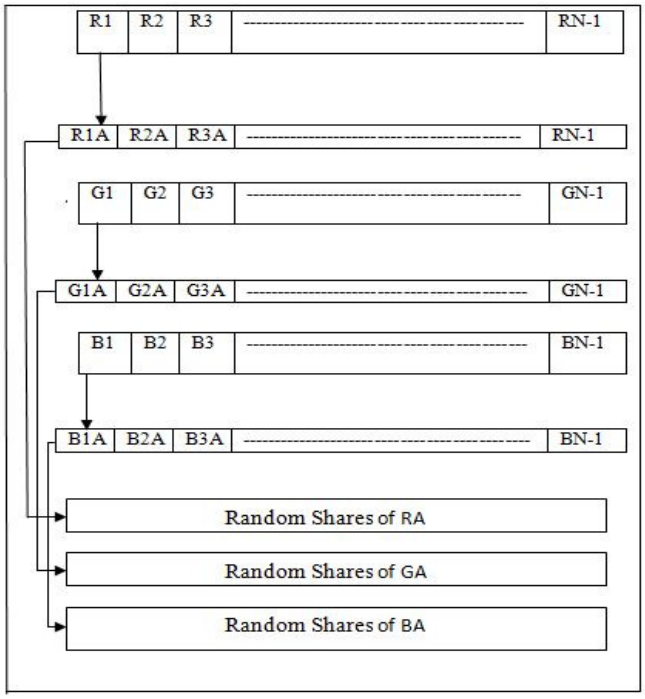

Fig. 3. Model diagram of Division

IV. PERFORMANCE DISCUSSION

In the proposed system the application doesn't use key management. The combined image and data encrypted and decrypted by using SDS algorithm. As this encryption algorithm encrypts image with data while decrypting get the lossless image and data. The main purpose of this paper is to avoid the attackers by using the visual cryptography. In this scheme sieving, division and shuffling the images into two shares, when they are try to login they should enter the valid code then only it will allow the user to the original page

V. CONCLUSION

Maintaining the secrecy and confidentiality of images is a vibrant area of research. Divide the image into random shares to maintain the images secrecy. The random shares so generated individually convey no information about the secret image then cover an encrypted share by a greyscale image, however to recover the original image all the random shares would be required. Image with data transferred from one end to other end by wireless sensor where data is encrypted into image is done by without using key. Storing the image with data and sending both at a time. As it's a less time consuming and process completes in a faster way, the original secret image recovered completely. It is implemented with the SDS algorithm.

REFERENCES

[1] SANS Institute InfoSec Reading book, SANS institute infosec reading room site, www.sans.org, © SANS Institute 2001

[2] F.Liu,C.K.Wu,X.J.Lin," Colour Visual Cryptography Schemes", Eighth International Conference On Intelligent systems Design And Applications Of Computer Society , Ieee2008.

[3] Lee Shu-Teng Chen, Wei-Kai Su, And Ja-Chen Lin," Secrete Image Sharing Based On Vector Quantization", International Journal Of Circuits, Systems And Signal Processing, Issue 3, Volume 3, 2009.

[4] Shiuh-Jeng Wang, I-Shuan Lin, Lin-Chun Lin, And Wen-Ya Chiang," A Secret Sharing Authentication 2009 Scheme For Digital Images", Journal Of Computers Vol.20, No.1, April

[5] Yuh-Ren Tsai, Pin-You Chen2, And Chien-Chih Shen," A Scheme Of Image-Based Signature Verification Upon Secret Sharing For Shopping In E-Commerce S Ystems", 15 July 2009

[6] Chin-Chen Chang, Chia-Chen Lin, And Huynh Ngoc Tu," Safeguarding Visual Information Using (T, N) Verifiable Secret Shares", Wwwg.Tw/Journ.Csroc.Org 26 June 2010, P. 89-96

[7] Adel Hammad Abusitta," A Visual Cryptography Based Digital Image Copyright Protection", Pp. 96104, 2010

[8] Manikandan R," Reversible Data Hiding For Encrypted Image", Journal of Computer Applications Volume-5, Issue 2012, February 10, 2012

[9] Dr.D.Nalini And A Pg Student W.Cantida," Hiding a Secret Image as Multiple Share using visual cryptography and stenography", International journal of innovative research and studies In april 2013, volume 2, Issue 4

[10] C.Anuradha and S.Lavanya," Secure and Authenticated Reversible Data Hiding In Encrypted Image", International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 3, Issue 4, April 2013

[11] Siddharth malik, Anjali sardana and Jaya "A keyless approach to image encryption", International conference on communication systems and network technologies,Ieee 2012.

[12] Geetha C.R. and Dr.Puttamadappa C., "Modified Weighted Embedding Method For Image Steganography" International journal of Electronics and Communication Engineering &Technology (IJECET), Volume 4, Issue 3, 2013, pp. 154 - 161, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472