An Enhanced VCS of Image Encryption using SDS algorithm without secret keys

Kanchana M V [1]
II[nd] year M-Tech
Department of CS&E
National Institute Of Engineering
Mysore, India
kanchana.306@gmail.com

Annapurna V K [2]
Associate Professor, Department of CS&E
National Institute Of Engineering
Mysore, India
annu_purna_i@yahoo.com

Abstract : An appropriate approach that can enable image encryption and decryption efficiently is formulated in this survey. Maintaining the secrecy and confidentiality of images is a vibrant area of research. Image encryption basically follows two different approaches, the first being encrypting the images through encryption algorithms using keys, the other approach involves dividing the image into random shares to maintain the images secrecy. The limitation of first approach is heavy computation cost and key management issues. Similarly the poor quality of the recovered image from the random shares limit the applications of the second approach. A different approach to image encryption is encrypting the images without the use of secret keys. In this paper the approach of image encryption using the concept of sieving, dividing and shuffling is described. It can be analyzed that with this new approach being implemented, random shares can be generated with minimal computation, with no pixel expansion and the original secret image can be recovered from the random shares without any loss of image quality. *This scheme is robust to withstand brute force attacks.*

Keywords : *Visual Cryptography, Pixel sieve, Chaotic algorithm, Sieving, Shuffling, Random shares, SDS.*

*****

1. INTRODUCTION

Using internet, transmission of audio, video and image is increasing rapidly. So the security of the transmitted data becomes mandatory. Cryptography is the desired technique to provide security. There are two processes in cryptography. Encryption is the first process in which the plain text or readable text is converted into cipher text or unreadable text. The second process is called decryption process in which the cipher text or unreadable text is converted to plain text or readable text. To encrypt data, an encryption algorithm is used at the sender , to reveal the data at the receiving end, a decryption algorithm is used. To make some applications cost effective, the decryption algorithms are avoided in many situations. One such area is the encryption in VC (Visual cryptography) using encryption algorithm where there is no need of decryption algorithm to reveal the visual information. Here the decryption process is done simply by human visual system. During the encryption process simply add some noise in the original image to hide the original information and during the decryption process the noise is reduced. The Encryption mainly concentrates on hiding the data based on some of the algorithms. The algorithms can deal with the concept of public and private key encryption. Both techniques have different sets of the algorithms and have their own advantages and disadvantages. At any instant of time in internet the number of file accesses is uncountable. Loss of data either by intruder or an hacker is more, so providing security is compulsory and mandatory over the network. This paper concentrates more on the image secrecy without keys. Encryption of images are broadly classified into lossless and lossy encryption [7]. There are studies on image encryption using the keys with digital signatures [1], chaos theory [2] and vector quantization. These techniques have some drawbacks that they are limited with the key size and high computation and also weak security. To overcome all these limitations the concept of VC was developed which involves secret sharing of image by dividing it into multiple shares. An hacker cannot perceive any clues about a secret image from individual random share images, as the visual cryptography involves the multiple shares. In this scheme the individual shares convey no information because the splitting takes place at the pixel level but the qualified set of these shares will help to regenerate the original image [3].

Technology has changed the world dramatically. Last few decades have witnessed some great events especially in the field of digital communication. In this paper characterization of different image encryption algorithms based on their properties is provided. The advantages of these algorithms and their demerits are also discussed. Image encryption algorithms are generally evaluated on performance measure such as contrast, security, accuracy, computational complexity etc.

Section 2 gives the existing system, Section 3 describes the proposed technique followed by applications, results and future work in Section 4, 5 and 6 respectively.

ISSN: 2321-8169
1794 – 1798

2. EXISTING SYSTEM

2.1 ENCRYPTION AND DECRYPTION PROCEDURE USING DIGITAL SIGNATURE

The digital signature of the original image is added to the encoded version of the original image. The encoding of the image is done using an appropriate 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. An optical correlation, in either the Joint Transform Correlator (JTC) or the Vander Lugt geometry, or digital correlation technique, can be used to verify the authenticity of the decrypted image. The digital signatures have some disadvantages such as high dependency on the technology it is based on. In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates and verification software from trusted certification authorities. There are many different digital signature standards and most of them are incompatible with each other and this complicates the sharing of digitally signed documents. Encryption and decryption procedure is shown in fig 1 and 2 below.[1]

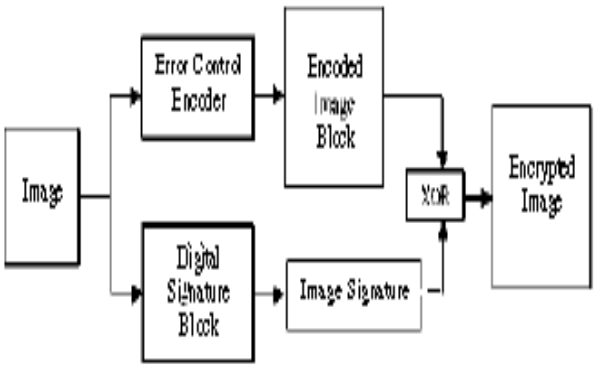

Fig 1 The block diagram of the encryption procedure using DS

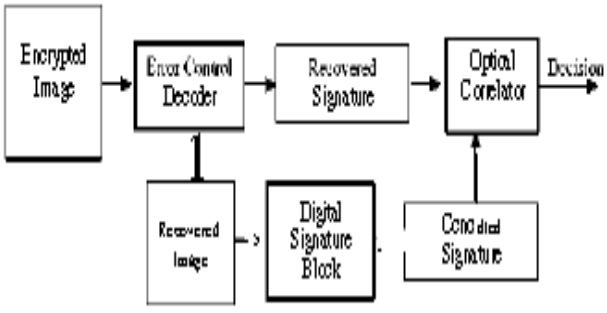

Fig 2 The block diagram of the decryption procedure using DS.

2.2 CHAOS THEORY

A new image encryption algorithm was introduced based on Henon chaotic maps in order to meet the requirements of the secure image transfer. There are several parameters in this kind of chaos system, and it is sensible to the original value and unpredictable. The results of several experimental, statistical analysis and key sensitivity tests show that the proposed image encryption scheme based on Henon chaotic maps provides an efficient and secure way for image encryption. The distribution of grey values of the encrypted image has a random-like behavior[2]. The limitation of applying chaos theory is choosing the input parameters. The methods chosen to compute these parameters depend on the dynamics underlying the data and on the kind of analysis intended, which is in most cases highly complex and not always accurate.The fig 3 below shows the chaotic encryption algorithm implemented.

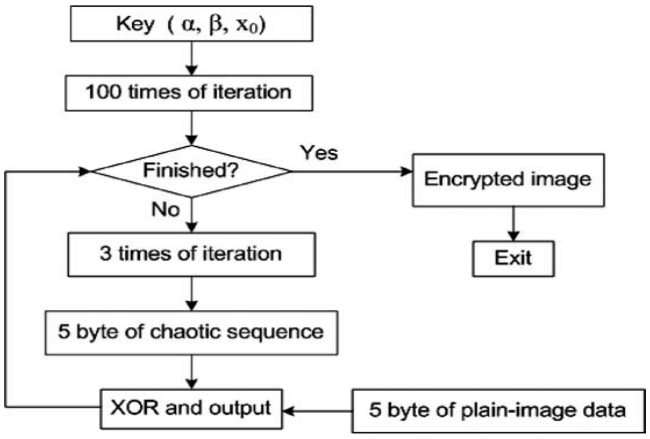

Fig 3 Block diagram of the chaotic encryption algorithm.

2.3 SHARED KEY

Shared key algorithm works directly in the JPEG domain, thus enabling shared key image encryption for a variety of applications. The scheme directly works on the quantized Discrete Cosine Transforms (DCT) coefficients and the resulting noise-like shares are stored in the JPEG format. The decryption process is lossless preserving the original JPEG data. The experiments indicate that each share image is approximately the same size as the original JPEG image retaining the storage advantage provided by JPEG compression standard. There are three extensions given in the paper , one to improve the random appearance of the generated shares, another to obtain shares with asymmetric file sizes, and the third to generalize the scheme for n>2 share cases.[14]. A hacker can listen to the unencrypted and the encrypted challenge, and extract the shared key from this information. When a hacker knows the shared key, the whole authentication mechanism is compromised and the hacker can access the WLAN network. This is the major disadvantage with Shared Key Authentication.

2.4 PIXEL SIEVE METHOD

Visual cryptography encodes a secret image into *n* shares which are distributed to n participants. Pixel Sieve method

 ISSN: 2321-8169
1794 – 1798

was proposed recently to encode an image into shares, but the encryption quality is poor. Based on cross merge and key shifting schemes, it generates quite noisy and highly secure encrypted images. Pixel sieve method is used to reduce the chances for an attacker to guess the secret using keys which are nearly equal to the original key. The new method can be broadly used in a number of visual secret sharing applications which requires high quality secret images and high security such as electronic cash, secret maps etc.

The original image is placed over the key sieve. The pixels of the original image which are situated above the holes in the sieve go through and form one share. The remaining pixels form the other share of the image. The method is illustrated in the Fig 4.

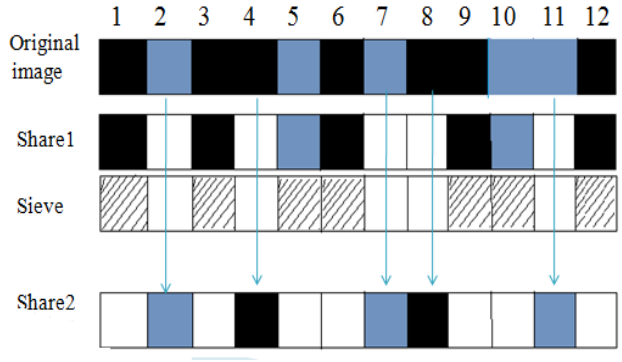

Figure 4 An example of pixel sieve method

There are some inherent limitations with all the above techniques implemented in the existing system- 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 with weak security functions are also an issue [5].

The related work corresponds to the working of image encryption and splitting of the image for security purposes. There can be the combination of splitting and encryption which results in the hybrid approach, which is applied for the SDS algorithm [3]. The idea of Image splitting involves the splitting of the secret image into n random shares such that these shares individually reveal no information about the secret image. The random image shares printed on transparencies and stacked up revealing the original image.

3. PROPOSED TECHNIQUE

Proposed technique involves splitting an image into multiple shares. The shares so generated reveal no information about the original secret image and to retrieve the secret image all the shares are required. The proposed technique is implemented with the SDS algorithm and involves three steps and is explained further in detail.

In step one (Sieving) the secret image is split into primary colors. In step two (Division) these split images are randomly divided. In step three, these divided shares are then shuffled each within itself. Finally these shuffled shares are combined to generate the desired random shares. The scheme that we present here is a (z, z) threshold scheme i.e. for retrieving a secret image that has been divided into z shares all z shares are required. No shares individually convey any information about the secret image, nor do a combination of subset of random shares, the original image will only be retrieved from the complete set of random shares. The scheme implemented using the SDS (Sieve, Division, and Shuffle) algorithm involves the following three steps:

Sieving: Sieving involves filtering the combined RGB components into individual R, G and B components. The granularity of the sieve depends on the range of values that R/G/B component may

take individually. To make the process computationally inexpensive, sieving uses the XOR operator.

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.

R→ (RA, RB, RC, ----------, RZ)

G → (GA, GB, GC, ----------, GZ)

B → (BA, BB, BC, ----------, BZ)

Shuffle: 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 color. 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.

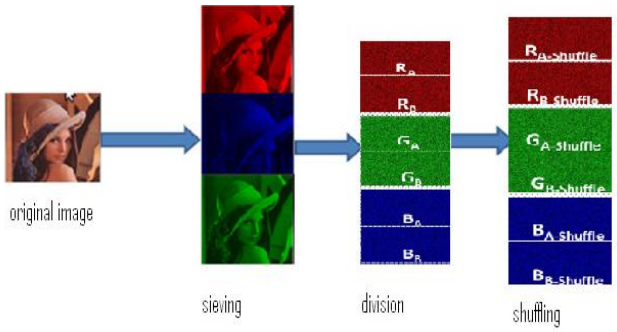

Fig 5 Steps showing SDS process

The random shares so generated individually convey no information about the secret image, however to recover the original image all the random shares would be required.

Overall system design is explained with data flow diagrams in fig 6 both for Encryption and Decryption and the system architecture in fig 7 provides an overview of system implementation and steps followed.

 ISSN: 2321-8169
1794 – 1798

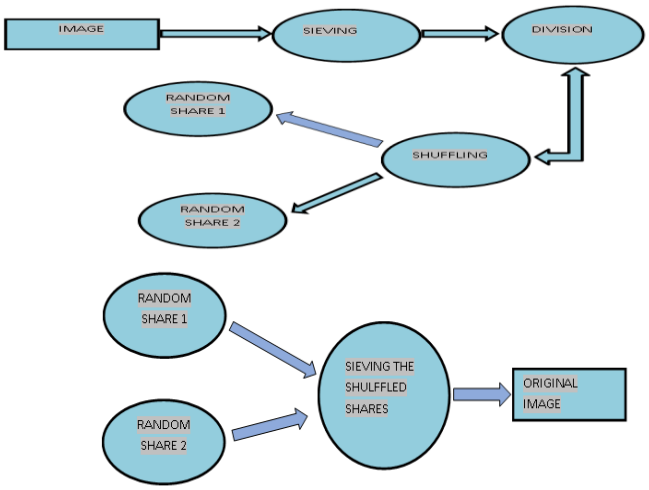

Fig 6 DFD for both Encryption and Decryption

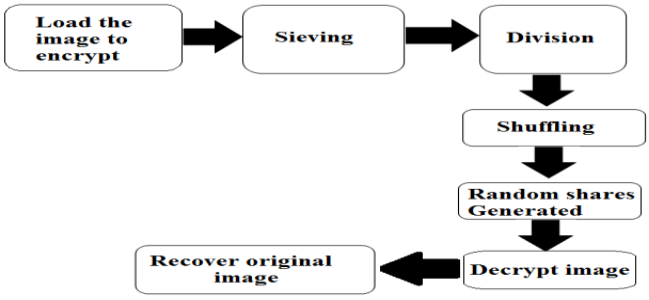

Fig 7 System Architecture

4. APPLICATIONS

Today the growth in the information technology, especially in computer networks such as Internet, Mobile communication, and Digital Multimedia applications such as Digital camera, handset video etc. has opened new opportunities in scientific and commercial areas.

(a) Developers: Keyless approach can be used to email the secret images to any recipient, so that no intermediate nodes can hack it, in between LAN.

(b) Military: It is also used for military purpose, a typical scenario for this could be thought of as a secret code which has to be fed into nuclear strike, the said code could be converted into an image spilt into random shares, held with the collective decision making body. To retrieve the secret code random share of all the participants would be required. They use this kind of technique in order to share secret images of some terrorist or officers or some blast photos.

(c) Banking: Many banking websites provide individual to select their own security image when creating their account for subsequent login. The image is displayed along with the caption. If they do not see the image and the caption they choose, they are instructed not to login.

5. RESULTS AND CONCLUSION

To validate SDS algorithm a modified (2,2) threshold VCS has been implemented. A photograph of a user could be clicked and divided into Z shares. In all the existing techniques explained the quality of the recovered image is almost similar to the original secret image, however the fact remains that the recovered image is not same as the original secret image. In this scheme the recovered image is an exact replica of the original image as no data is lost during the sieving division and shuffling operations. The results were validated using Normalized Correlation (NC). NC is used to measure the correlation between the original secret image and the recovered images from the random shares. The NC for all the recovered images was 1.0 for multiple images. Hidden messages can also be encrypted and decrypted along with an image [2]. Cryptograghy techniques which includes both encryption and decryption by various methods are understood and described in table 1.

In this paper a new enhanced visual cryptographic scheme is described, which is a hybrid of the traditional VCS and the conventional image encryption schemes. The algorithm does not use the traditional approach of using an encryption key; but definesa SDS algorithm for encrypting an image. A secret image is split into multiple random images and with minimum computation the original secret image can be retrieved back.

6. FUTURE WORK

The following can be implemented in the future.

(a) Improving the encryption facility with multiple images simultaneously.

(b) Compressing shares before transmission so less storage space across intermediate nodes is used.

(c) At the destination end, a buffer may be added to determine how long each random share of an image need to be maintained until all shares are received.

REFERENCES

[1] Aloka Sinha and Kehar Singh, *"A technique for image encryption using digital signature"*, Optics Communications (2003), 218(4-6), pp 229-234,online [http://eprint.iitd.ac.in/dspace/handle/2074/1161]

[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] Malik, S. ;Sardana, A. ; Jaya, J.*"A Keyless Approach to Image Encryption"*, Communication Systems and Network Technologies (CSNT), 2012 International Conference on Digital Object

Identifier:10.1109/CSNT.2012.189Publication Year: 2012 , Page(s): 879 - 883

[4] Sudharsanan, S.“Shared key encryption of JPEG color images”, Consumer Electronics, IEEE Transactions on Volume: 51 , Issue: 4 Digital ObjectIdentifier:10.1109/TCE.2005.1561845 Publication Year: 2005 , Page(s): 1204 – 1211.

[5] Arpad Incze, “Pixel sieve method for secret sharing & visual cryptography” RoEduNet IEEE International Conference Proceeding Sibiu 24-26 June 2010, ISSN 2068-1038, p. 89-96

[6] R. Lukac, K.N. Plataniotis “Bit-level based secret sharing for image encryption”, The Journal of Pattern Recognition Society, 2005.

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

[8] 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.

[9] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin , “Sharing A Secret Two-Tone Image In Two Gray-Level Images”, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.

[10] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multiple-Image Encryption By Rotating Random Grids”, Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[11] F. Liu1, C.K. Wu X.J. Lin , “Colour Visual Cryptography Schemes”, IET Information Security, vol.2, No. 4, pp 151-165, 2008.

[12] Du-Shiau Tsai , GwoboaHorng , Tzung-Her Chen , Yao-Te Huang , “A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint”, Information Sciences 179 3247–3254 Elsevier, 2009.

[13] 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.

[14] C.C. Thien, J.C. Lin, “Secret image sharing”, Computers & Graphics, Vol. 26, No. 5, 2002, pp. 765-770.

Table 1 Comparison of Survey process

Paper	***A technique for image encryption using Digital signature***	***A new chaotic algorithm for image encryption***	***Shared key encryption of JPEG color images***	***A keyless approach to image Encryption***
Technology	Based on Digital signature	Based on Henon Chaotic maps	Works on quantized DCT coefficients	Implemented with SDS algorithm
Working	DS of the original image is added to the encoded version of the original image	Based on the non linear systems and mapping	Encryption is done inside the DCT coefficient	It employs Sieving, Division and Shuffling
Computational speed	Faster Computation speed	Average computation speed	Low computation speed	Computation speed faster
Key transmission	No need to transmit key	Key need to be transmitted to receiver	Key need to be transmitted to receiver	Keyless approach
Security	Secure	Secure	Weak security	More secure