IJCAT - International Journal of Computing and Technology
Volume 1, Issue 1, February 2014
www.IJCAT.org

A Survey of Image Encryption Using Different Approaches

[1] C. Sebastian Sneha, [2] Hannah Jose, [3] Jismi K Jacob, [4] Diana Davis

[1, 2, 3] Information Technology Department, University of Calicut,
Jyothi Engineering College, Cheruthuruthy
Thrissur, Kerala, India

[4]Assistant Proffessor, Dept. of Information Technology,
Jyothi Engineering College, Cheruthuruthy,
Thrissur, Kerala, India

Abstract - This is a survey to formulate the appropriate approach that can enable image encryption efficiently .Image Encryption basically follow 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. First approach is being limited as heavy computation cost and key management is an issue and 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 encryption keys. It can be analyzed that with this new approach being implemented random shares can be generated with minimal computation and the original secret image can be recovered from the random shares without any loss of image quality.

Keywords **- Visual Cryptography, Sieving, Shuffling, Random shares.**

1. Introduction

The Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. With dawn of internet introduced to its users a whole new dimension as to how data can be shared from one part of the world to the other in near real time. However along with these opportunities came the challenges, such as, how to maintain the confidentiality of the data being transmitted. This gave a fillip to the already vibrant research area of cryptography.
.
"Digital signatures" [1], 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. Detailed simulations have been carried out to test the encryption technique. An optical correlate, in either the JTC or the Vander Lugt geometry, or digital correlation technique, can be used to verify the authenticity of the decrypted image.

"Chaos Theory" [2], a new image encryption algorithm is presented 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.

"Shared Key" [3], is a shared key algorithm that works directly in the JPEG domain, thus enabling shared key image encryption for a variety of applications. The scheme directly works on the quantized DCT coefficients and the resulting noise-like shares are also 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. Three extensions, 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, are described as well.

"Keyless Approach" [4] can be implemented with the SDS algorithm and involves three steps. 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 (Shuffling) these divided shares are then shuffled each within itself. Finally these shuffled shares are combined to generate the desired random shares.

2. Image Encryption Techniques

2.1 Image Encryption (using keys)

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" [1], "Chaos Theory" [2], "Vector Quantization" [3] 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. However the greatest strength of most of these schemes is that the original image is recovered in totality.

2.2 Image Splitting

This approach, in a very basic form, involves splitting an image at the pixel level into multiple shares (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). Adi Shamir [6] in 1979 is credited for introducing the idea of dividing a secret data into 2 random shares. In 1995, Naor and Shamir [7], 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 [7] have been researched to overcome its limitations, each having their own merits and demerits. Despite the advancements made in this line of research, the quality of the recovered secret images still remains an area of concern due to the poor quality of these recovered images (including loss of contrast and colors). Despite its limitations the greatest strength of these schemes is that firstly, there is no requirement of key management and secondly the decryption involves no computation.

To overcome the limitations of existing two approaches we propose a new scheme, through which the quality of the recovered image is maintained. In addition, this scheme does not involve use of keys for encryption, has low storage and bandwidth requirements, while also keeping the computation cost during encryption/ decryption low.

3. Literature Survey

Image Encryption means that, convert the image into unreadable format. Digital visual data is organized into rectangular arrays-frames. Elements of array are denoted as pixel. Each pixel is a numerical value.

In "Digital Signatures" [1], the digital signature issued to encrypt the message by adding it, bit-wise, to the encoded version of the original image. The digital signature is treated like additive noise, which can be recovered at the receiver end. To be able to recover the digital signature, an error control code is used to encode the original image. An error control code takes in the original image and adds redundancy in a known manner so that the bits corrupted by noise can be recovered. In our case, the digital signature is the noise that is added to the image after error control coding. The addition operation is equivalent to the XOR operation. We have used the BCH error control code to encode our original image. The original image is used to compute the digital signature. The image is then encoded using an appropriate BCH code. The digital signature is added block wise to the encoded image. The resulting image is the encrypted image.

"Chaos Theory" [2], the image encryption algorithm includes two steps. Firstly, the image fusion is completed between the original-image and the key-image. Then the pixel values of the fusion-image are encrypted by Henon chaotic system.

"Shared key" [3], the scheme directly works on the quantized DCT coefficients and the resulting noise-like shares are also stored in the JPEG format. The decryption process is lossless preserving the original JPEG data. Monochrome Images: The lossy version of JPEG image compression uses discrete cosine transforms (DCT). A monochrome image is first split into 8×8 non-overlapping blocks of pixels. An 8×8 DCT is applied to each block and the resulting coefficients are scalar quantized using a quantization matrix. The quantized coefficients are then converted from a two-dimensional representation to a one-dimensional vector by a process known as zigzag

scanning and sent to an entropy coder that uses either Huffman or arithmetic coding.

Color Images and JPEG Modes: This scheme uses the same JPEG approach to handle color images. Since the resulting image shares are JPEG images, any color space that can be handled by JPEG is also suitable for our application. JPEG supports up to 255 components in one image and hence support for a large variety of image formats.

Paper name	***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 signaturing	Based on Henon chaotic maps	Works on the quantized DCT coefficients	Implemented with the SDS algorithm
Working	DSS of the original image is added to the encoded version of the original image	Based on 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 tranmission	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

Table 1: Comparison of survey papers

4. Proposed Technique

Our 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.

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 various steps involved in generating two random shares are depicted in Figure 1.

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.

$R \rightarrow (R_A, R_B, R_C, \text{----------}, R_Z)$
$G \rightarrow (G_A, G_B, G_C, \text{----------}, G_Z)$
$B \rightarrow (B_A, B_B, B_C, \text{----------}, B_Z)$

While dividing it is ensured that each element in R_{A-Z}, G_{A-Z} and B_{A-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.

Shares so generated should be such that (R_A, R_B, R_C, ---------- R_Z) should regenerate R and similarly for G/B components.

Shuffling: Though experimental results have shown that 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. R_{A-Z}, G_{A-Z} and B_{A-Z} , we perform the shuffle operation. 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 R_B decides how R_A is shuffled, R_C decides how R_B is shuffled, ---------- R_Z decides R_Z-1 is shuffled and R_A 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).

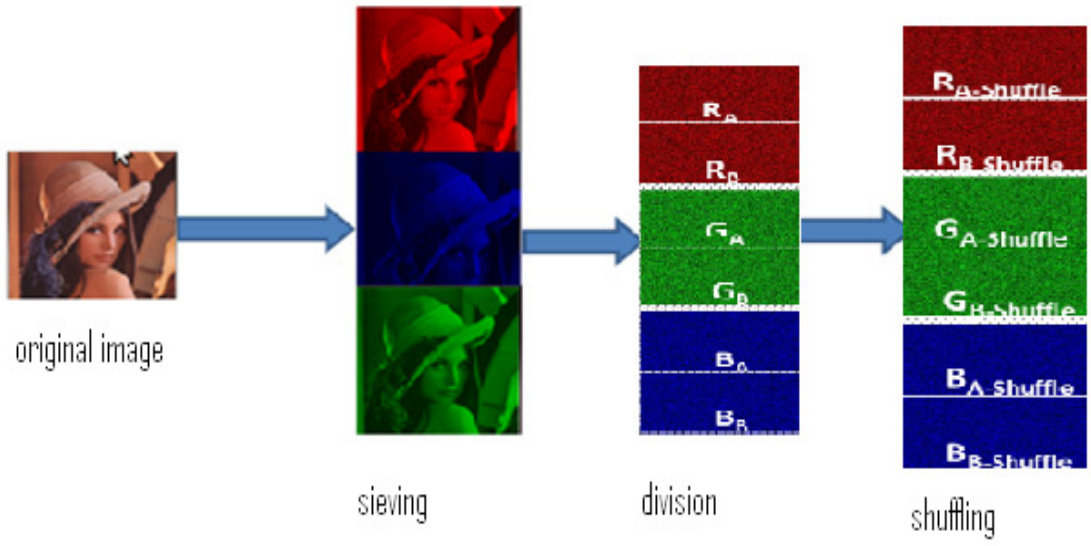

Fig 1: Steps involved in encryption

$RS_A \rightarrow$ (R_A- shuffle, G_A- shuffle and B_A- shuffle)
$RS_B \rightarrow$ (R_B- shuffle, G_B- shuffle and B_B- shuffle)
- - - -
$RS_Z \rightarrow$ (R_Z, - shuffle G_Z- shuffle and B_Z- shuffle)

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.

5. Conclusion

In this paper a new enhanced visual cryptographic scheme is presented, which is a hybrid of the traditional VCS and the conventional image encryption schemes. A secret image is split into multiple random images and with minimum computation the original secret image can be retrieved back. The proposed algorithm has the following merits (a) The original secret image can be retrieved in totality (b) There is no pixel expansion and hence storage requirement per random share is same as original image (c) Key management is not an issue since there are no secret keys involved as encryption is carried out based on the distribution of values amongst various shares (d) the scheme is robust to withstand brute force attacks.

The scheme is suitable for authentication based application or where trust cannot be reposed in any one participant for decision making and a collective acceptance is required to proceed. A typical scenario for this could be thought of as a secret code which has to be fed in to commence a nuclear strike; the said code could be converted into an image and split into random shares,

held with the collective decision making body. To retrieve the secret code random share of all the participants would be required.

Reference

[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.2012.189 Publication 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 Object Identifier: 10.1109/TCE.2005.1561845 Publication Year: 2005 , Page(s): 1204 – 1211.

[5] S.Behnia, A.Akhshani, S.Ahadpour, H.Mahmodi,A. Akha-van,"A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,"Physics Letters A 366(2007):391-396.

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

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

[8] 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

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

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

[15] 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.

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