World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:1, No:3, 2007

Analysis and Comparison of Image Encryption Algorithms

İsmet Öztürk[1] and İbrahim Soğukpınar[2]

[1, 2]Gebze Institute of Technology Computer Engineering Dept. 41400 Gebze /Kocaeli

[1]ismetoz@hotmail.com, [2]ispinar@bilmuh.gyte.edu.tr,

Open Science Index, Computer and Information Engineering Vol:1, No:3, 2007 publications.waset.org/13928.pdf

***Abstract*—** With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access. In this paper, we analyzed current image encryption algorithms and compression is added for two of them (Mirror-like image encryption and Visual Cryptography). Implementations of these two algorithms have been realized for experimental purposes. The results of analysis are given in this paper.

***Keywords*—**image encryption, image cryptosystem, security, transmission.

I. Introduction

THE field of encryption is becoming very important in the present era in which information security is of utmost concern. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

In order to transmit secret images to other people, a variety of encryption schemes have been proposed. Schemes that we analyze here can be classified into three major types: position permutation [4]-[5], value transformation [1]-[2]-[3]-[6] and visual transformation [4].

A study of image compression is becoming more important since an uncompressed image requires a large amount of storage space and high transmission bandwidth. In this paper we have proposed new schemes which add compression capability to the mirror-like image encryption [4] and visual cryptography [7] algorithms.

The rest of this paper is organized as follows. Current image encryption schemes are introduced briefly in section two. In Section three, we compare these encryption algorithms with each other and propose our compression schemes. Section four contains experimental results. Final section is conclusions.

II. Image Encryption Algorithms

A. A Technique for Image Encryption using Digital Signatures

Aloka Sinha and Kehar Singh [1] have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by 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.

B. Lossless Image Compression and Encryption Using SCAN

S.S. Maniccam and N.G. Bourbakis [2] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves.

C. A New Encryption Algorithm for Image Cryptosystems

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [3] use one of the popular image compression techniques, vector quantization to design an efficient cryptosystem for images. The scheme is based on vector quantization (VQ), cryptography, and other number theorems. In VQ, the images are first decomposed into vectors and then sequentially encoded vector by vector. Then traditional cryptosystems from commercial applications can be used.

D. A New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture

Jiun-In Guo and Jui-Cheng Yen [4] have presented an efficient mirror-like image encryption algorithm. Based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm. This algorithm consists of 7 steps. Step-1 determines a 1-D chaotic system and its initial point $x(0)$ and sets $k = 0$. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates binary sequence from chaotic system. Steps-4,5,6, and 7 rearrange image pixels using swap function according to the binary sequence.

Open Science Index, Computer and Information Engineering Vol:1, No:3, 2007 publications.waset.org/13928.pdf

E. A New Chaotic Image Encryption Algorithm

Jui-Cheng Yen and Jiun-In Guo [5] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point *x(0),* row size *M* and column size *N* of the image *f,* iteration number *no,* and constants *α, β,* and μ used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels. These functions are;

- $ROLR_l^{i,p} : f \to f'$ is defined to rotate each pixel in the *i*th row in *f,* $0 \le i \le M-1$, in the left direction *p* pixels if *l* equals 0 or in the right direction *p* pixels if *l* equals 1.
- $ROUD_l^{j,p} : f \to f'$ is defined to rotate each pixel in the *i*th column in *f,* $0 \le j \le N-1$, in the up direction *p* pixels if *l* equals 0 or in the down direction *p* pixels if *l* equals 1.
- $ROUR_l^{k,p} : f \to f'$ is defined to rotate each pixel at position *(x,y)* in the image *f* such that *x+y=k,* $0 \le k \le M+N-2$, , in the upper-right direction *p* pixels if *l* is equal to 1 or in the lower-left direction *p* pixels if *l* is equal to 0.
- $ROUL_l^{k,p} : f \to f'$ is defined to rotate each pixel at position *(x,y)* in the image *f* such that *x-y=k,* $-(N-1) \le k \le M-1$, in the upper-left direction *p* pixels if *l* is equal to 0 or in the lower-right direction *p* pixels if *l* is equal to 1.

F. Color Image Encryption Using Double Random Phase Encoding

Shuqun Zhang and Mohammad A. Karim [6] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green-Blue) formats. The proposed single-channel color image encryption method is more compact and robust than the multichannels methods.

G. Visual Cryptography for Color Images

Visual cryptography uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Young-Chang Hou [7] have proposed three methods for visual cryptography.

Gray-level visual cryptography method first transforms the gray-level image into a halftone image and then generates two transparencies of visual cryptography. Obviously, we indeed cannot detect any information about the secret image from the two sharing transparencies individually, but when stacking them together, the result clearly shows the secret image.

Method 1 uses four halftone images, cyan, magenta, yellow and black, to share the secret image. The codes of the four sharing images are fully disordered, and we cannot perceive any clue of the original secret image from any single sharing image. Method 2 reduces the inconvenience of Method 1 and requires only two sharing images to encrypt a secret image. However, after stacking the sharing images generated by Method 2, the range of color contrast will be 25% of that of the original image. Method 3 loses less image contrast, which is better than Method 2.

III. Comparison and Proposed Method

A. Comparison of current algorithms

A brief comparison of image encryption schemes is given in Table I. Also detailed properties of each method are introduced following.

Image Encryption using Digital Signatures [1] algorithm encrypts the image and embeds the digital signature into the image prior to transmission. This encryption technique provides three layers of security. 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. The dimension of the image also changes due to the added redundancy. This poses an additional difficulty to decrypt the image. Also, the digital signature is added to the encoded image in a specific manner. At the receiver end, the digital signature can be used to verify the authenticity of the transmitted image. The advantage of the scheme is the authenticity verification. Increment in the size of the image due to added redundancy is the disadvantage of the algorithm. Also it does not have any compression scheme.

The algorithm which uses SCAN language [2] has lossless image compression and encryption abilities. The distinct advantage of simultaneous lossless compression and strong encryption makes the methodology very useful in applications such as medical imaging, multimedia applications, and military applications. The drawback of the methodology is that compression-encryption takes longer time.

Mirror-like image encryption algorithm [4] and chaotic image encryption algorithm [5] are similar in nature. Both algorithms use binary sequence generated from the chaotic system to rearrange an image pixels. These algorithms do not have any compression scheme and authenticity verification. However they do lossless image encryption-decryption which makes images to be in a chaotic state very quickly.

Major advantage of the algorithm which is proposed by Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [3] has a simple hardware structure. Required bit rate of VQ is

TABLE 1: PROPERTY COMPARISON TABLE

Algorithm	Compression	Loss	Authenticity
IEDS	No	No	Yes
SCAN	Yes	No	No
MIE	No	No	No
CIE	No	No	No
VQ	Yes	No	No
DRP	No	No	No
VC	No	Yes	No

IEDS – Image Encryption using Digital Signatures
SCAN - *Lossless Image Compression and Encryption Using SCAN*
MIE – Mirror-like Image Encryption
CIE – Chaotic Image Encryption
VQ - *A New Encryption Algorithm for Image Cryptosystems*
DRP- *Color Image Encryption Using Double Random Phase Encoding*
VC - *Visual Cryptography for Color Images*

small. Since VQ compresses the original image into a set of indices in the codebook, we can save a lot of storage space and channel bandwidth. The other advantage is that VQ has a simple hardware structure for providing a fast decoding procedure.

Color Image Encryption Using Double Random Phase Encoding [6] technique introduces color information to optical encryption. An *RGB* color image is converted to an indexed image before it is encrypted using a typical optical security systems. At the decryption end, the recovered indexed image is converted back to the *RGB* image. Since only one channel is needed to encrypt color images, it reduces the complexity and increases the reliability of the corresponding optical color image encryption systems.

The most notable feature of the visual cryptography for color images approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography. Also, the contrast of the stacked image is somewhat downgraded, but the content of the image can still be easily identified.

B. Adding compression to MIE and VC algorithms

We have compared the MIE and VC algorithms. Results are given in Table II and III. Also enhancements which are shown in Fig.1 and Fig. 2 have been done on the MIE and VC algorithms by adding compression ability to them. In the new enhanced scheme encrypted images are compressed by either loss or lossless compression algorithms before transmission to the destination.

We have modified MIE algorithm so that it can reduce the disk storage space and network bandwidth. Before transmission encrypted image is compressed with the compression algorithm. At the receiver end compressed image is decompressed and then decrypted. Also compression is added for visual cryptography. Visual cryptography produces 2 sharing images for gray-level images, 4 sharing images for method1, 2 sharing images for method2 and method3. Compression is more important issue for visual cryptography because it produces 2 or more sharing images which are twice in size of dimensions of the original image.

TABLE II: ENCRYPTION – DECRYPTION DURATION

Algorithm	Image	Encryption (s)	Decryption (s)
MIE	Lena (grayscale)	0.27	0.22
MIE	Lena (color)	5.00	5.16
MIE	Baboon (grayscale)	0.49	0.22
MIE	Baboon (color)	9.23	9.23
VC	Lena (grayscale)	1.98	- *
VC	Lena (color)	4.56	- *
VC	Baboon (grayscale)	3.57	- *
VC	Baboon (color)	8.35	- *

TABLE III: MEMORY USAGE

Algorithm	Image	Encryption (bytes)	Decryption (bytes)
MIE	Lena (grayscale)	1114209	1114193
MIE	Lena (color)	1245293	1245275
MIE	Baboon (grayscale)	2082593	2082581
MIE	Baboon (color)	2327605	2327591
VC	Lena (grayscale)	4784488	-*
VC	Lena (color)	24576306	-*
VC	Baboon (grayscale)	8942856	-*
VC	Baboon (color)	45937802	-*

* Visual cryptography exploits the human visual system to read the secret message from some overlapping shares.

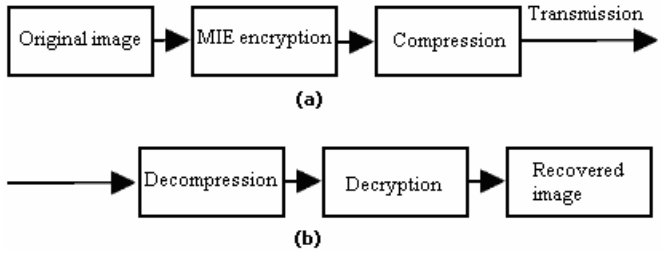

Fig. 1. New MIE (a) at sender end (b) at receiver end

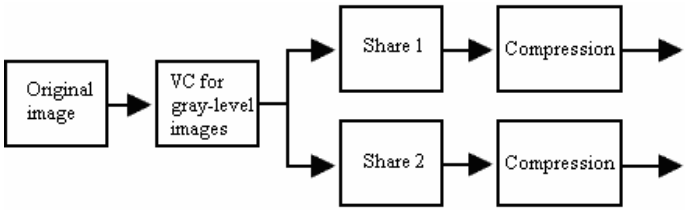

Fig. 2. New VC for gray-level images encryption

JPEG (Joint Photographic Experts Group) is a standard compression algorithm used to reduce memory requirement for the storage of digital images. The JPEG standard allows to specify the desired quality of the encoded image by varying a quality factor between 0 (lowest quality) and 100 (best quality).

PNG is an extensible file format for the lossless, portable, well-compressed storage of raster images. While the jpeg compression has losses in the compressed image, in PNG compression there is neither a change of colors nor a reduction of color depth.

Mean square error (MSE) is the cumulative squared error between original and recovered image. Lower value of MSE means lesser error. Formula for MSE is:

Open Science Index, Computer and Information Engineering Vol:1, No:3, 2007 publications.waset.org/13928.pdf

$$MSE = \frac{1}{N.M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[|f(i,j) - f'(i,j)|^2] \quad [8]$$

Where *f(i,j)* is the original image and *f'(i,j)* is the compressed image value.

IV. Experimental Results

A. Experiment Environment

In this paper image processing software package (MATLAB) is used as the engine for the image processing experiments. An RGB image is stored in MATLAB as an *M*-by-*N*-by-3 data array that defines red, green, and blue color components for each individual pixel. The color of each pixel is determined by the combination of the red, green, and blue intensities stored in each color plane at the pixel's location.

Images that are used during these experiments are uncompressed images and listed in Table IV.

B. Results

Image properties and results of the experiments are presented in Table IV and V.

TABLE IV :Image Properties

Image	Dimensions	s.b.	s.a.MIE	s.a.VC *-**
Lena (gray)	256x256	65536	65536	2x 262144
Lena (color)	256x256x3	196608	196608	4x 786432
Baboon (gray)	350x350	122500	122500	2x 490000
Baboon (color)	350x350x3	367500	367500	4x 1470000

* - VC produces 2 sharing images twice in dimensions of the original image for gray-level encryption

** - VC produces 4 sharing images twice in dimensions of the original image for color image encryption Method1

s.b. – Size before encryption (bytes)

s.a.MIE – Size after MIE encryption (bytes)

s.a.VC – Size after VC encryption (bytes)

V. Conclusions

In this work MIE and VC algorithms have been improved by adding compression capability. As we can see from the experimental results jpeg with quality parameter set to 100 does not compress grayscale image, besides size of the grayscale image increases, because noise in the image can not be compressed productively. Quality setting set to 90 or below reaches good compression ratios. However jpeg is not suitable for color images (even with quality set to 100) because of the loss in the color. Thus PNG lossless compression is ideal for color image compression with MIE. VC is not a lossless encryption in nature, thus compression algorithm have to chosen carefully. Lossless PNG compression for gray-level and color images has a big compression ratio because it has only one color plane to encrypt and saves storage space and network bandwidth up to 91,4%.

TABLE V: RESULTS

Alg.	Image	C.A.	C.S.(bytes)	Ratio (%)	MSE
MIE	Lena (gray)	J100	88532	132,9	5.52e-005
MIE	Lena (gray)	J90	42584	63,9	0.000336
MIE	Lena (gray)	PNG	63939	95,9	1.24e-005
MIE	Lena (color)	J100	116650	59,3	0.000392
MIE	Lena (color)	J90	49653	25,2	0.000558
MIE	Lena (color)	PNG	190674	96,9	4.59e-005
MIE	Baboon (gray)	J90	75941	61,1	0.000336
MIE	Baboon (gray)	PNG	116336	93,6	7.59e-005
MIE	Baboon (color)	J90	94470	25,6	0.0166
MIE	Baboon (color)	PNG	362311	98,3	0.000271
VC	Lena (gray)	J90	2x 185014	70,5	- *
VC	Lena (gray)	PNG	2x 35355	13,4	- *
VC	Lena (color)	J90	4x 173106	22,0	- *
VC	Lena (color)	PNG	4x 68856	8,7	- *
VC	Baboon (gray)	J90	2x 349797	71,3	- *
VC	Baboon (gray)	PNG	2x 64583	13,1	- *
VC	Baboon (color)	J90	4x 327861	22,3	- *
VC	Baboon (color)	PNG	4x 127712	8,6	- *

C.A. – compression algorithm, C.S. – compressed size

Ratio – Compression ratio, MSE – Mean square error.

J100 – Jpeg compression algorithm with quality parameter set to 100

J90 – Jpeg compression algorithm with quality parameter set to 90

* - MSE can not be computed for VC algorithm because of the difference on the dimensions between original image and produced shares.

References

[1] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, 2003, 1-6

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

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

[4] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce

[5] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm",Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China, *E-mail:* jcyen@mail.lctc.edu.tw

[6] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", MICROWAVE AND OPTICAL TECHNOLOGY LETTERS / Vol. 21, No. 5, June 5 1999, 318-322

[7] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition 36 (2003), www.elsevier.com/locate/patcog, 1619-1629

[8] Amhmed Saffor, Kwan Hoong Ng, Abdul Rahman bin Ramli, David Dowsett, "A Comparison of JPEG and Wavelet Compression Applied to Computed Tomography Brain, Chest, and Abdomen Images", The Internet Journal of Medical Simulation and Technology, ISSN:1540-2657, www.ispub.com

Open Science Index, Computer and Information Engineering Vol:1, No:3, 2007 publications.waset.org/13928.pdf