SECURITY OF E-MAIL ATTACHMENT BY USING CHAOS [+]

السرية في ارتباطات البريد الالكتروني باستخدام الفوضى

Walid A. AL-Hussaibi [*]

Abstract:

Continuously security becomes more important than ever. The rise of e-mail capabilities has increased the need for caring about security aspects. The protection is traditionally designed according to the worth of obtainable information. Thus, security is by far one of the main components and one of the biggest challenges in e-mail attachments. Using computer simulation a new technique of security is used in e-mail attachment by using chaos. Computer programme is designed to convert the attachment file(s) (Word, Excel, Power point, Images, Pdf, …) to PDF file. By this programme each page of the PDF file is converting to a single image called page-image. A mask-image is generated with the same size of each image using manipulated data extracted from nonlinear dynamical system (chaotic system), which has high sensitivity to initial conditions. Each pixel of the mask-image is added to the analogue pixel of the page-image to produce jamming-image. All jamming-images are then converted to one secret PDF file to send it as e-mail attachment file with a compression ratio of more than 10% in size . In the receiving end after downloading of secret attachment file, a real number of password with 12 digits must be interred correctly in order to open the secret PDF file by the same programme. The mask-image will be generated again for each jamming-image in decoding process. High level of security was achieved by this method. The precision of this method is very high up to 10^{-12} for each password and it can be used also in many applications in the field of mobile communications.

المستخلص:

تزداد أهمية الأمان بتقدم الوقت. إن تنامي قدرات البريد الالكتروني زادت من الحاجة إلى الاهتمام بمستلزمات الأمان. إن الحماية تصمم اعتمادا" على مستوى أهمية المعلومات المتوفرة. هكذا، فان الأمان وعلى المدى البعيد يبقى من المكونات الرئيسية واحد اكبر التحديات في مجال الارتباطات بالبريد الالكتروني. باستخدام المحاكاة بالكومبيوتر تم إيجاد تقنية جديدة للامان في ارتباطات البريد الالكتروني باستخدام الفوضى. تم تصميم برنامج كومبيوتر لتحويل ملفات الارتباط (..., Word, Excel, Power point, Images, Pdf) إلى ملف PDF . باستخدام هذا البرنامج كل صفحة في ملف PDF تحول إلى صورة منفردة تسمى صورة-الصفحة. يتم توليد صورة-القناع بنفس الحجم لكل صورة باستخدام بيانات معالجة ومستخرجة من نظام حركي غير خطي (نظام فوضوي) والذي يمتلك حساسية عالية للشروط

[+] Received on 1/10/2007 ,Accepted on 6/8/2009 .

[*] Lecturer/ Technical College of Basrah

الابتدائية. كل نقطة من صورة–القناع تجمع مع النقطة المناظرة لها في صورة–الصفحة لإنتاج صورة–التشويش. كل صور–التشويش تحول بعد ذلك إلى ملف PDF سري واحد لكي ترسل كملف ارتباط بالبريد الالكتروني بنسبة ضغط بالحجم أكثر من 10%. عند طرف الاستلام وبعد تحميل ملف الارتباط السري، يجب إدخال الرقم السري المتكون من ١٢ رقم حقيقي بصورة صحيحة لكي يقوم نفس البرنامج بفتح الملف السري. صورة القناع يتم تولدها مجددا" لكل صورة–تشويش في عملية فك الشفرة. بهذه الطريقة تم الحصول على مستوى عالي من الأمان. إن دقة هذه الطريقة عالية جدا" تصل إلى 10^{-12} لكل كلمة سر ويمكن استخدامها ايظا" لعدة تطبيقات في مجال الاتصالات للهواتف النقالة.

Introduction:

Internet and wireless communications are advancing rapidly. Millions of peoples are used the facility of e-mail via internet services at any minute. They communicate with each others and transfer a lot of data files as e-mail attachment [1]. We are currently on the verge of a new revolutionary advancement in wireless data communications, the third generation of mobile telecommunications 3G promises to converge mobile technology with Internet connectivity. Wireless data and integrated services will be among the major driving forces behind 3G. While wireless communications provide great flexibility and mobility, they often come at the expense of security. This is because wireless communications rely on open and public transmission media that raise further security vulnerabilities in addition to the security threats found in regular wired networks [2].

At the beginning of the 1920s image were coded with five brightness levels then it was increased to fifteen in 1929 [3]. Since then, the demand for images in digital form has increased steadily for better resolution. Subsequently the amount of information required for storage or transmission of an image increased. Effective image coding and/or compression (loss less or lossy) became a necessity to allow for short transmission time or reasonable storage space. This led to a variety of image coding and compression models in use and development today [4, 5, and 6]. On the other hand, the most exciting recent developments in nonlinear dynamics are the realization that chaos can be useful. It is effectively unpredictable periodic long-term behavior in deterministic system that exhibits sensitive dependence on initial conditions with noise like spectrum. Since about 1990, people have found ways to exploit chaos to do some marvelous and practical things such as private/secret communications [7, 8].

Message masking in private communication can be applied using a computer simulation of chaotic system such as double scroll oscillator [9]. The mask of chaotic signal is added at the transmitter to the message. To recover the original message at the receiver, the received signal is used for synchronization and to regenerate the masking signal then subtract it from the received signal.

Many researchers have been trying to study the image coding/compression techniques where a hybrid image coding based on partial fractal mapping is applied [10]. Only part of the image can be encode using fractal technique and model the remaining part using other algorithms. Nonlinear wavelet transforms for image coding are presented in [11]. Researchers in [12] describe efficient sign coding for embedded wavelet image coding where the wavelet transform coefficient are defined by both a magnitude and sign.

Suppose you want to send a secret /important file by e-mail attachment, naturally you should use a code, so that even if enemy found it, he will have trouble to know the fact. This is an old problem. People have been making (and breaking) codes for as long as there have been secrets worth keeping. Thus, this paper is focused on security of e-mail attachment by the use of new coding technique with compression ratio more than 10%. It is organized as follows, the next section describe the new technique. Third Section, demonstrate generation of the mask-image from nonlinear dynamical system data and in the forth section, simulation results are given for secret file coding and decoding. Finally, some conclusions and recommendations are withdrawn from this paper.

The New Security Technique in Attachment Files:

Through this section we investigate the new technique method of secret e-mail attachment file coding. Suppose you want to send a private file(s) (Word, Excel, Power point, Image, Pdf, …) via e-mail on your computer with high security. This new technique use a computer programme which makes a links with MATLAB 6.5 and Adobe Acrobat R&W 6.0 Professional programs to insure your order.

The main idea is to make a conversion for each type of attachment file to Pdf file as a first step. After that each page of the Pdf file is converted to JPEG image called page-image. The total number of page-images equal to the number of pages in the Pdf file. Coding process is made for all page-images by using chaos. Mask-image is generated from nonlinear dynamical system data after some manipulation. The properties of mask-image are similar to page-image; it has the same size (pixels), same class (unit8, unit16, or double arrays), same colormap (hsv, hot, pink, gray...) and the same extension format (jpeg). This image has a form depend on the initial condition of the system then any slight change in initial condition produce another image form (some times can not recognized by eyes). For any page-image with it's mask-image each pixel will be encoded by adding with the analogues pixel to produce another image called the jamming-image. The total number of jamming-images is equal to page-images in the Pdf file. The programme make the last step by convert all the jamming-images to one Pdf file with extension of (.pdf). This file can be send as attachment e-mail with compression in size approximately more than 10% and high level of security. In the receiving end, after downloading your secret e-mail attachment, the program told you to enter the password when you need to open the Pdf file. The password represents the initial conditions of the nonlinear system that's used in this program. If the password is correct; The Pdf file is converted from (.pdf) extension to (.jpeg) extension to get the jamming-images. The same generation of the mask-images will be repeated to subtract it from the jamming-images. After subtraction and processing the result will be the original page-images. These recovered page-images are converted again to (.pdf) extension format. In other side if an intruder tries to have your secret file by entering invalid password the result will be jamming-images again. This is because of the beautiful property of the nonlinear dynamical systems which is the high sensitivity to initial conditions. Different nonlinear dynamical systems with different initial conditions give a flexibility to use from one to another.

Mask-image generation*:*

The nonlinear dynamical system that is used to generate the mask-image through this paper is the double hook attractor (for more details see [13]) which is described by:

$$dx/dt = (G/C_1)(y-x) - (1/C_1)\,[m_o x + 0.5(m_1 - m_o)|x+Bp| + 0.5(m_o - m_1)\,|x-Bp|]$$
$$dy/dt = (G/C_2)(x-y) + z/C_2 \quad (1)$$
$$dz/dt = -y/L$$

Where: $x = Vc_1$, $y = Vc_2$, $z = i_L$, $C_1 = -0.0647$, $C_2 = 0.3180$, $L = -0.3005$, $G = 0.5390$, $Bp = 1$, $m_o = -0.5013$ and $m_1 = -1.3475$.
Data matrix of three columns and 30000 rows is the result of solving equation (1) using computer simulation with initial conditions: $x(0)=0.01$, $y(0)=0$, $z(0)=0$ (you can choose

any other values because it represents the password) and total number of iterations are 30000. The *x* state is represented by the first column in this matrix while *y* and *z* states are represented by second and third columns in the data matrix respectively. Since the data matrix contains a real numbers then, MATLAP program is used to make some data manipulations at the first step such as:

- *Absolute value*: to remove any negative sign of the data matrix elements.
- *Scaling*: to improve pixels intensity values (fixed by the program designer).
- *Quantization*: to remove the fractals of data matrix elements.

In the second step, image of data matrix (mask-image) will be formed from the manipulated nonlinear system data matrix according to properties of page-image that we need it. The number of data elements that we used in the image data matrix is limited by the page-image size only. But if it is not enough then the program makes more iteration to increase the nonlinear system data matrix elements. Mask-image then will be generated from the image data matrix and saved with (.jpeg) extension. Fig.(1) represent manipulated *200* data point of a segment of *y*-state after absolution, scaling by *25* and quantization.

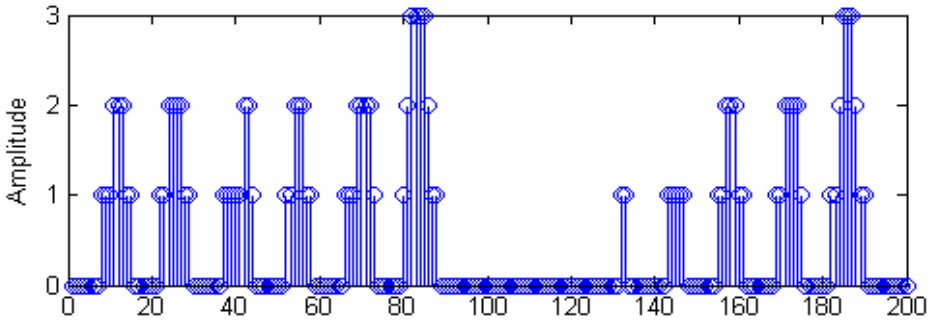


Fig.(1): manipulated *200* data point of a segment of *y*-state after absolution, scaling by *25* and quantization**.**

A mask-image of *gray* colormap, *jpeg* extension format, size of *256X256* pixel , *65536* bytes and class *uint8* array is represented in Fig.(2-a) . This noisy image is a signature to the nonlinear dynamical system with given initial conditions. Any slight changes in initial conditions (password) change the locations of black and white pixels in the image then produce another image (but some times you can't see the difference by your eyes). This property makes high difficulties for the intruder to break the code. Image histogram of the mask-image is represented in Fig.(2-b) where the extreme black and white intensity is dominated in class *uint8* over all the contrast potential range from zero to *256* and it can be easily controlled by the program designer to get a good jamming result.

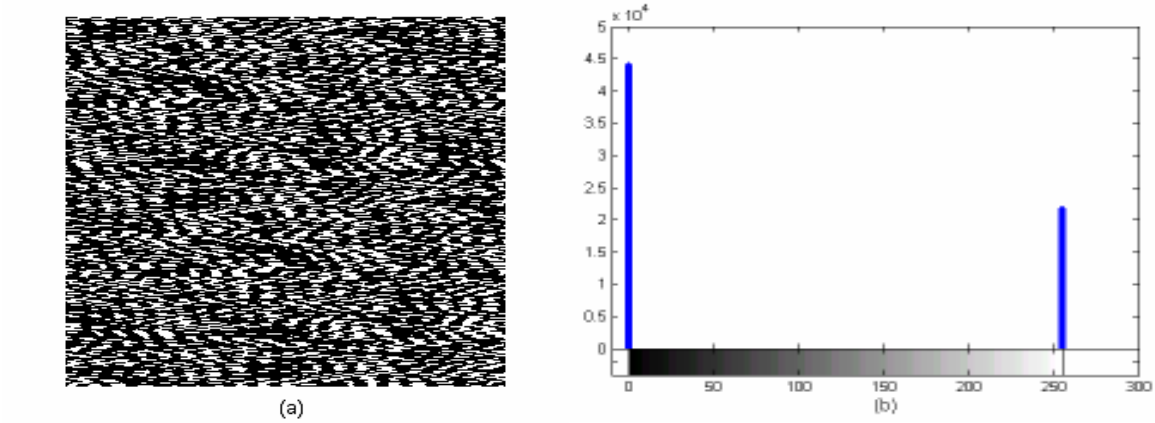


Fig.(2): a- Mask-Image generated from manipulated nonlinear dynamical system data.
b- Image histogram

The generated mask-image above will be used in the next section for secret e-mail attachment coding and decoding.

Simulation of security of e-mail attachment files:

To illustrate performance of our method using computer program, example of attachment files will be taken with the following properties:

1- File name: *F1.pdf ,* Size: *137 Kbyte ,* Type: *Adobe Acrobat document with one page.*
2- File name: *F2.doc ,* Size: *27 Kbyte ,* Type: *Microsoft Word document with one page.*
3- File name: *F3.jpeg,* Size: *15.2 Kbyte,* Type: *Image (gray colormap).*
4- File name: *F4.ppt,* Size: *13 Kbyte ,* Type: *Power Point Presentation with one slide.*

These files are to be used in a secret e-mail attachment. The total size of these files is *192.2Kbyte*. For transmission security, the next subsection describes the coding procedure.

1- **Coding Procedure:**

1- Start the designed computer program by entering your password, which is contains 12 digit real number as (**********).
2- Browse the files into program one by one.
3- The programme converts all files to one PDF file with (.pdf) extension.
4- Convert all pages of the PDF file to images called page-images (each page converted to single image with JPEG extension).
5- Generate mask-images with same number and properties of page-images (one to one).
6- Scaling factor is multiplied with both two images (for each pair; mask-image and page-image) to avoid image saturation in the image addition step.
7- Applying image addition for each pair of images to create the jamming-image, which has the same properties of the above two images. The number of jamming-images is equal to page-images.
8- Create a final PDF file (secret file) with (.pdf) extension from all jamming-images.
9- Save the final PDF file (secret file) with appropriate name. This file is ready now to send as a secret e-mail attachment.

Simulation results of page-images of our example are represented in Fig.(3), where: Fig.(3-a) represent the page-image of the Pdf file *F1* , Fig.(3-b) represent the page-image of the word file *F2* , Fig.(3-c) represent the page-image of the image file *F3* and Fig.(3-d) represent the page-image of the power point file *F4*. All of the mask-images that analogues to page-images are represented in Fig.(4). The jamming-images which is the result of addition of each pair (page-image and mask-image) are shown in Fig.(5). They are noisy images with a different contrast distribution and if you don't know the original images, then you can't recognize what these images represent at all. The final PDF file (secret file) which is created from all jamming-images consists of four (noisy) pages with total size of *173Kbyte*. For this example the total compression in size is 11%. The compression ratio depends completely on the type of original files. Image files are highly compressed than others. For e-mail attachments of image files only the compression in size reach high levels (approximately 85%). Fig.(6) represent the flowchart of e-mail attachment coding procedure.

(a): page-image of pdf file.

(b): page-image

(c): page-image of image file.

(d): page-image of

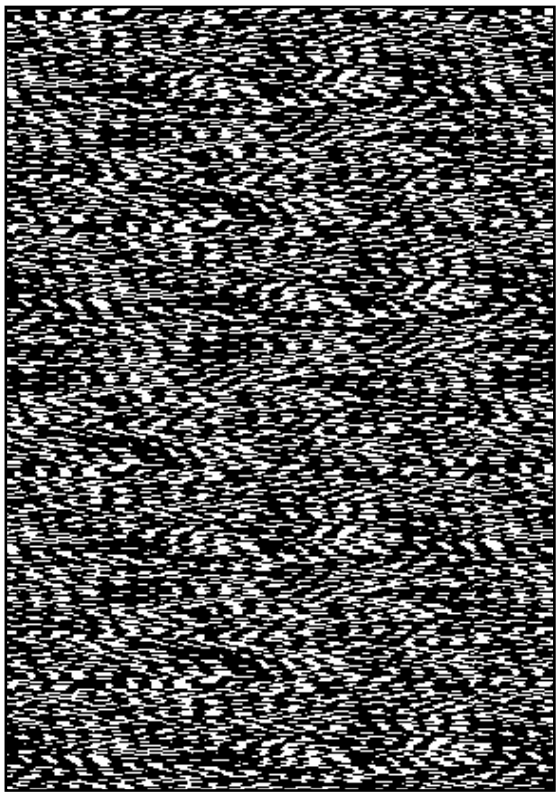
Fig.(3): Simulation results of page-images where:

(a) Represent the page-image of the Pdf file *F1*

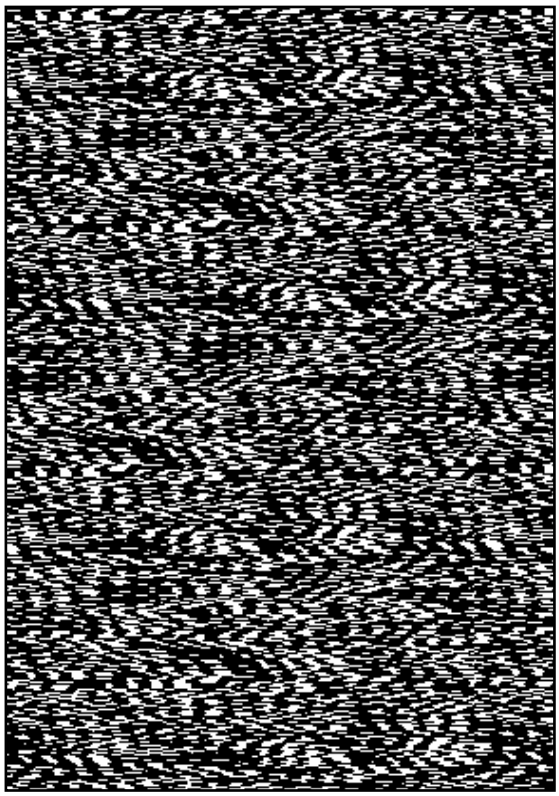
(b) Represent the page-image of the word file *F2*

(c) Represent the page-image of the image file *F3*

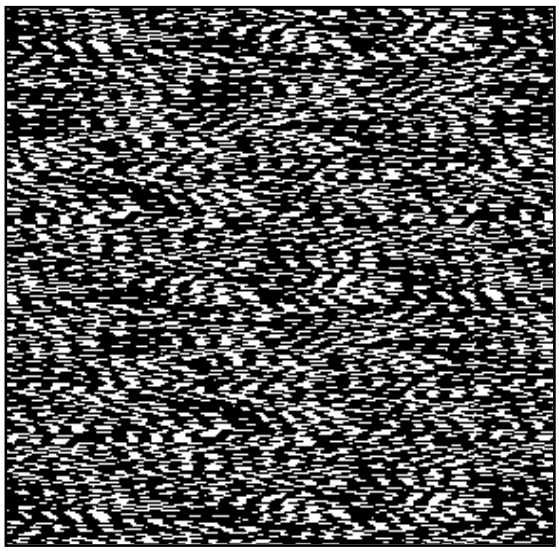
(d) Represent the page-image of the power point file *F4*.



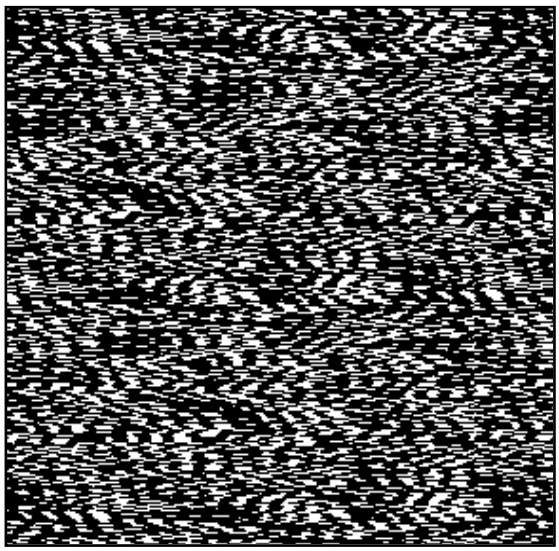
(a): mask-image of Pdf file



(b): mask-image



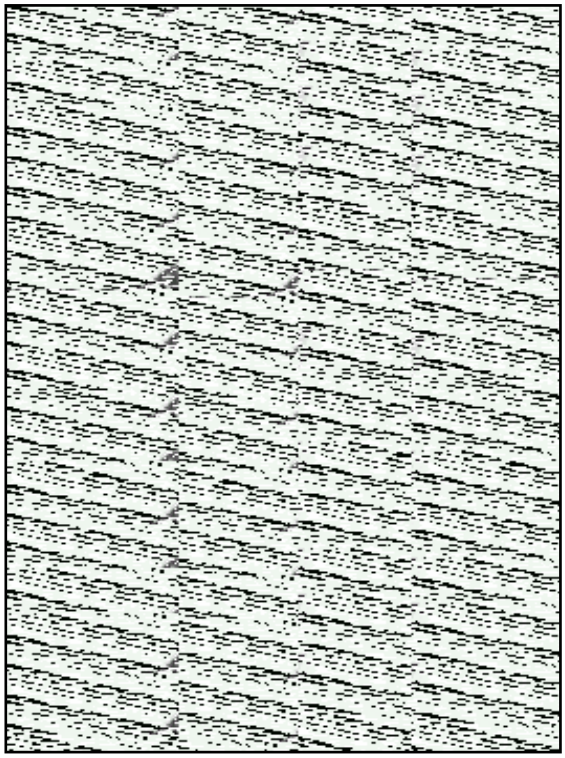
(c): mask-image of image file



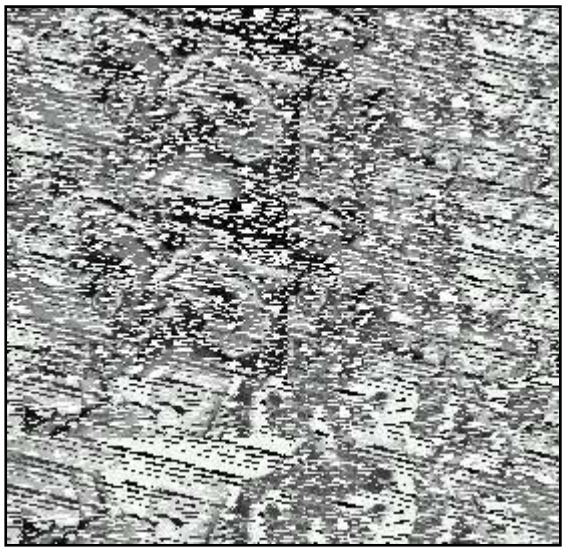
(d): mask-image of

Fig.(4): Simulation results of mask-images where:
(a) Represent the mask-image analogues to the page-image of Pdf file *F1*
(b) Represent the mask-image analogues to the page-image of word file *F2*
(c) Represent mask-image analogues to the page-image of image file *F3*
(d) Represent mask-image analogues to the page-image of power point file *F4*.

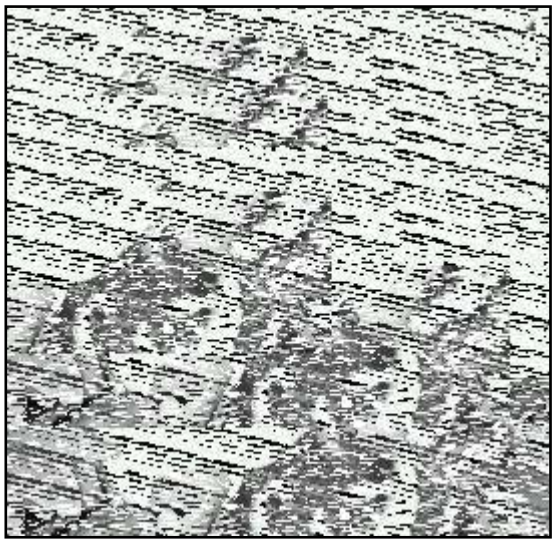
(a): jamming-image of Pdf file.



(b): jamming-image



(c): jamming-image of image file.



(d): jamming-image of

Fig.(٥): Simulation results of jamming-images where:

(a) Represent the jamming-image of the Pdf file *F1*

(b) Represent the jamming -image of the word file *F2*

(c) Represent the jamming -image of the image file *F3*

(d) Represent the jamming -image of the power point file *F4*.

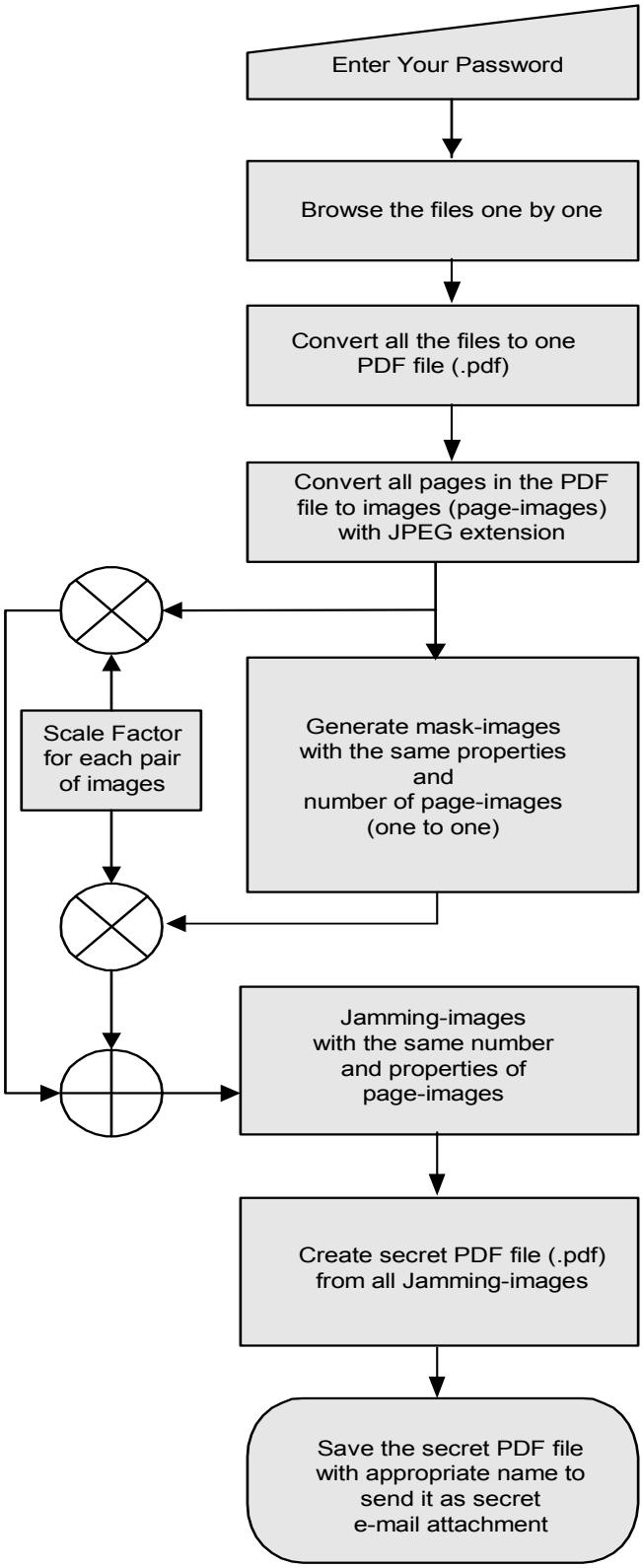


Fig.(6): Flowchart of e-mail attachment coding procedure.

Decoding Procedure:

In the receiving end when the PDF file (secret file) downloading occurred, no one can open it correctly only if the correct password entered. The following steps clarify the decoding procedure:

1. Start the same computer program by entering your password, which is contains 12 digit real number as (**********).
2. Load the PDF file (secret file) which has (.pdf) extension.
3. The programme converts all pages of the PDF file (secret file) to jamming-images (each page converted to single image with JPEG extension).
4. Generate mask-images with same number and properties of jamming-images (one to one).
5. Scaling factor is multiplied with both two images (for each pair; mask-image and jamming-image) for contrast improvement.
6. Applying image absolute subtraction for each pair of images (mask-image and jamming-image) to recover the original (un jammed) page-images.
7. Create a PDF file (received file) with (.pdf) extension from all page-images.
8. The output result is the original PDF file with perfect reconstruction.
9. If the password incorrect then, the output result is a secret PDF file again.

Simulation results of the recovered page-images of our example are represented in Fig.(7). A good image reconstruction are showed by this figure, it can't recognized by human eye from the original ones. What happens if an intruder tries to have your secret file? For incorrect password with up to 10^{-12} accuracy, the output is another secret file with jamming-images as shown in Fig.(8) It is also a noisy image with a different contrast distribution from the first jamming images. The change in password means that the initial conditions of the chaotic system are different, then the locations of black and white pixels in the generated mask-image is changed. Thus, the result of absolute subtraction is another jamming-image. Fig.(9) represent the flowchart of e-mail attachment decoding procedure. The user can decide the password of this program with its partner and changed it when they need.

3 The mobile phone form factors

VP4: Mobile positioning technologies and location services

Third-generation mobile communication systems (IMT-2000 and Universal Mobile Telecommunication System, UMTS) deliver voice, graphic, video, and other broadband information directly to the user, regardless of location, network, or terminal. Fourth-generation systems promise to extend this even further, providing integrated, seamless services over heterogeneous networks, with higher spectral efficiency and at lower price. The concept of context-awareness involves, to start with, the need to determine and deliver the geographic location of wireless terminals and devices to provide the personalized, customized service the user wants.

Mobile station (MS) location testing and verification have become an important issue for wireless carriers and the vendors. Since MS location information can be used for many location-dependent applications to enhance the system performance, there is also an explosive interest in the development of new location-based commercial services to add value to mobile devices. The ability to support position location within wireless networks provides network operators with additional value added services, as well as users with a host of new applications. This includes navigation, localization based services; network management and security applications.

This project examines the drivers and issues surrounding the development of location information from the wireless networks, independent of their air interfaces and positioning technologies, including the requirements for security, billing, and interoperability, in the context of a comparative analysis of existing and proposed location-positioning technologies and systems.

It also investigates the emergence of MS location commercial services and addresses how MS location information can be used (1) to improve performance of the systems through vertical layers, and (2) to increase wireless system functionality for location commercial services. Many factors influencing the choice for a positioning system are further analysed: from accuracy to impact on the handset and the network, cost and ease of integration.

(a)

(c)

Fig.(7): Simulation results of recovered page-images where:
(a) Represent the recovered page-image of the Pdf file *F1*
(b) Represent the recovered page-image of the word file *F2*
(c) Represent the recovered page-image of the image file *F3*
(d) Represent the recovered page-image of the power point file *F4*.

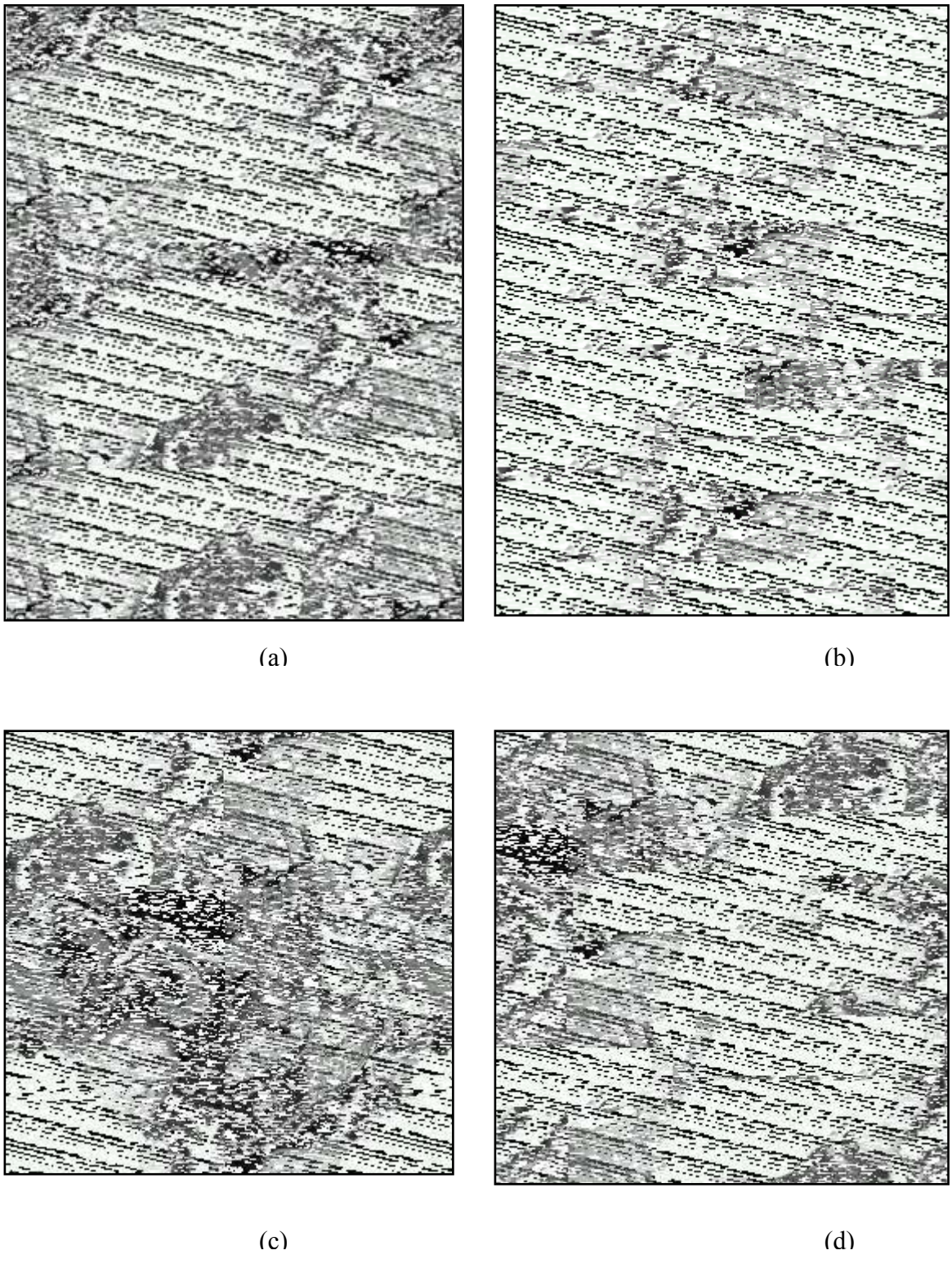


Fig.(8): Simulation results of recovered page-images for incorrect password where:
(a) Represent the recovered page-image of the Pdf file *F1*
(b) Represent the recovered page-image of the word file *F2*
(c) Represent the recovered page-image of the image file *F3*
(d) Represent the recovered page-image of the power point file *F4* .

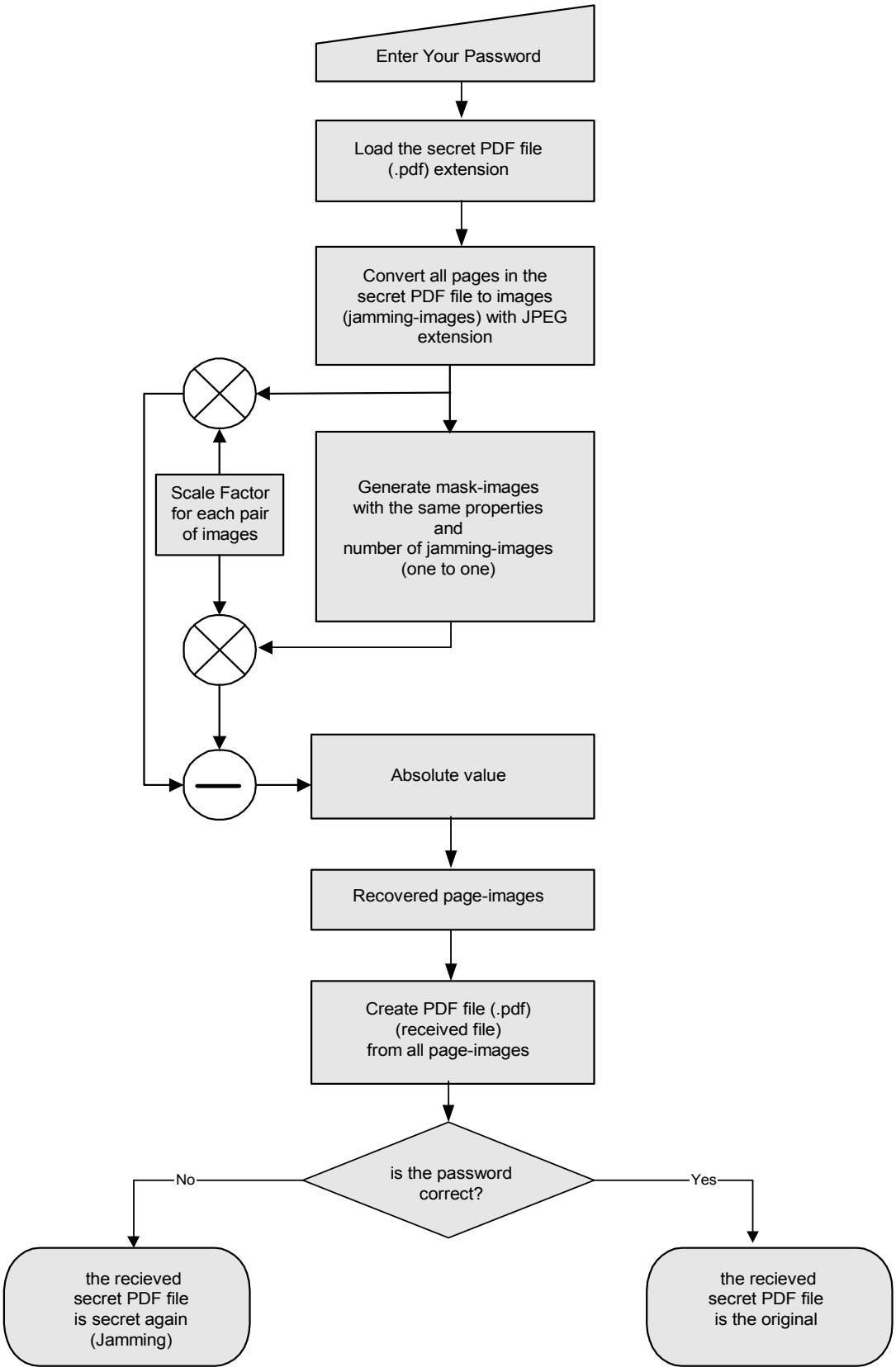

Enter Your Password
Load the secret PDF file
(.pdf) extension
Convert all pages in the
secret PDF file to images
(jamming-images) with JPEG
extension
Scale Factor
for each pair
of images
Generate mask-images
with the same properties
and
number of jamming-images
(one to one)
Absolute value
Recovered page-images
Create PDF file (.pdf)
(received file)
from all page-images
is the password
correct?
No
Yes
the recieved
secret PDF file
is secret again
(Jamming)
the recieved
secret PDF file
is the original

Fig.(9): Flowchart of e-mail attachment decoding procedure.

Conclusions:

We can use the nonlinear dynamics, which is very sensitive to initial conditions to build a complete computer programme for secret transmission of e-mail attachment files. Same program with same password must be used in order to open the desired files correctly. Complex password of real numbers (positive, negative, integer or fractal) make the probability of braking this programme extremely very low. There is no way to lose your private files if any one tries to steel, only if he knows the nonlinear system that's used and the required password. Good results are obtained from the simulation figures using the double hoock attractor. Acceptable compression ratio in the size of the files is obtained. It is depends on the type of the attachment files. There are many nonlinear dynamical systems, so you can choose any system for your program. Finally, we recommend developing this method for secret transmission of movie files in internet and mobile communications.

References:

[1] Kadner K., Yin M.," *Middleware support for context awareness in 4G environments*", Springer, 26-29, June 2006.

[2] Chebbine S., Obaid A., Johnston R., "*Framework architecture for internet content adaptation system and vertical handover management on 4G networks*" Wireless Telecommunication Symposium, 34- 44, April 2005.

[3] Rafael C. Gonzalez, Richard E. Wood, "*Digital Image processing*" , Addison-Wesley Publishing Company, 1993.

[4] S. Kumar, "*An Introduction to Image Compression*" , www.debugmod.com/imagecmp/ , 22 Oct, 2001.

[5] T. Karp, Pradeep Suthram, David Hemmert, " *Image Coding / Compression* " , A project paper for EE5364: Digital Signal Processing, spring 2002.

[6] K-G Stenborg, "*Function Coding of Images*", Department of electrical engineering, Linkoping University, Sweden , 2000.

[7] Steven H. Strogatz. "*Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry, and Engineering*". Addison-Wesley Publishing Company, second printing, November 1995.

[8] W. Al-Hussaibi, " *Effects of Low pass Filtering on Chaotic Signals of Boost Switching Regulators* ", The 8'Th Scientific Conference for foundation of technical education, 69-75, (2002).

[9] W. Al-Hussaibi, " *Masking of Messages Using the Double Scroll Attractor in Private Communications* ", 66-73, Volume 18 , No.2 , (2005).

[10] Z. Wang, D. Zhang and Y. Yu, *" Hybrid Image Coding Based on Partial Fractal Mapping "*, Signal Processing: Image Communication, 767-779, 15 (2000).

[11] R. Claypoole, G. Davis and W. Sweldens, *" Nonlinear Wavelet transforms For Image Coding "*, clayporl@ rice.edu, November 1997.

[12] A. Deever, Sheila S. Hemami, *" Efficient Sign Coding for Embedded Wavelet Image Coding "*, Cornell University, 2000.

[13] Leon O. Chua and Gui-Nian Lin, *" Canonical Realization of Chua's Circuit Family "*, IEEE Transaction. Circuits and Systems, Volume 37 , No.7 , July (1990)