ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

Android Application for Secret Image Transmission and Reception Using Chaotic Steganography

Savithri G[1], K.L.Sudha[2]

B.E, Dept of CSE, K.S. School of Engineering and Management, Bangalore, India.

Professor, Dept of ECE, Dayananda Sagar College of Engineering, Bangalore, India.

ABSTRACT: Information hiding is an art which has been used since long back for covert communication. Steganography is the art of hiding secret message within a larger image or a secret image in another cover image, such that the hidden message or an image is undetectable. Chaotic systems are known for its randomness, it can be made utilized in achieving the encryption. In this paper chaos-based encryption algorithm for images is used. This algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the pixels. Random pixel insertion method is used for hiding the secrete image in cover image. This Application is developed using the Java programming language in Android Software Development Kit. This application created for the Android operating system can be used in smart mobile phones for sending any image in a secrete manner by hiding it in another larger image.

KEYWORDS: Encryption, Steganography, Chaos, Android, Java

I. INTRODUCTION

The amazing developments in the field of network communications during the past years have created a great requirement for secure image transmission over the Internet. Internet is a public network and is not so secure for the transmission of confidential data. To meet this challenge, steganographic techniques need to be applied. In steganography a secret message/image is embedded in another image but change made in cover image will not cause visible changes in the cover image. Chaos is suitable for steganography, as it is closely related to some dynamics of its own characteristics. The behaviour of the chaos system, under certain conditions, presents phenomena which are characterized by sensitivities to initial conditions and system parameters. Through the sensitivities, the system responses act to be random. The main advantages of the chaotic steganographic approach include: Easy implementation, more randomness, sensitivity to initial conditions, non-periodic, and confidential. One of the simplest methods of steganography is random pixel insertion method wherein the scrambled pixels of the secrete image is inserted in a particular order in cover image. In this work, the message to be hidden is altered according to highly random chaotic sequence generated with Henon map. These pixels are inserted in the cover image in a periodic way such that no articrafts are seen in the cover image.

II. RELATED WORK

Thousands of papers which are based on steganography are available today. Individual papers deal with different algorithm to increase the secrecy in transmission. Papers which make use of chaos for cryptography uses different chaotic maps to generate random values and use these values to shuffle the pixels [papers 1-7]. To hide the encrypted image, LSB stuffing method is commonly used. DCT based steganography is another method to hide image [papers 8-11]. But the development of steganography application on android platform is considered to be more challenging as stated by authors of paper [12] “Steganography on a phone is more difficult, because it requires access to the device's operating system, but no one should doubt that committed individuals will have no trouble rising to the challenge”.

One of the most widely used mobile OS these days is **ANDROID**. Android is a software bunch, comprising not only operating system but also middleware and key applications. It is an open-source platform developed by Google and the Open Handset Alliance on which interesting and powerful new applications can be quickly developed and distributed to many mobile device users.[13,14] In this paper we have considered the development of the application on android platform.

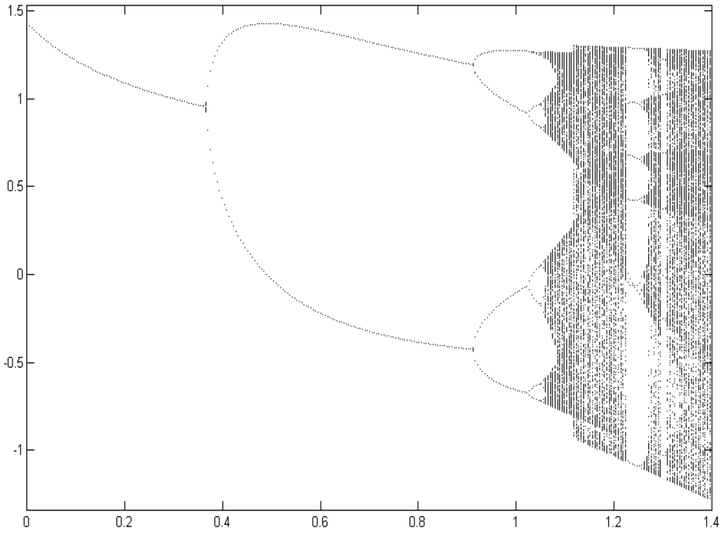
III. PROPOSED ALGORITHM

In the algorithm proposed, we consider two images, one is a cover image and another image is the secret image which has to be embedded in the cover image. The dimension of the secret image should be smaller than that of the cover image. The pixels ratio considered in the algorithm is 6:1.

Henon map is used to derive chaotic sequences, which is generated by using the equation

$$x_{n+1} = y_{n+1} - ax_n^{\,2},$$
$$y_{n+1} = b\,x_n \qquad \text{eq .(1)}$$

Here ‘a’ and ‘b’ are constants whose values are selected to get random sequence. Bifurcation map is helpful in selecting these values. In this application, we have used a =1.76 & b =0.1. If the secret image is an 80*80 image, a chaotic sequence of 6400 is produced taking some initial value for x_n where we get random region in the bifurcation map shown in figure(1). For Henon map, random region is found when initial value of x is considered in the range 1.1 to 1.4.



Figure(1) Bifurcation diagram of Henon Map

Chaotic maps are very sensitive to initial conditions. Even change in 5th decimal position gives a different sequence. Encryption algorithm is based on paper [7]. The chaotic values are arranged in ascending/descending order.

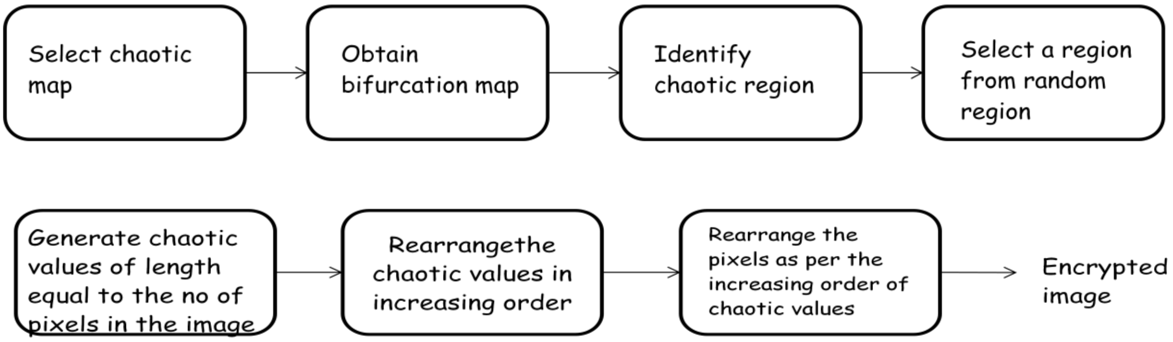
The pixels in the secret image are shuffled as per the order of replaced chaotic values to get scrambled image. The encryption process is illustrated in figure(2). With this we get first level of secrecy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

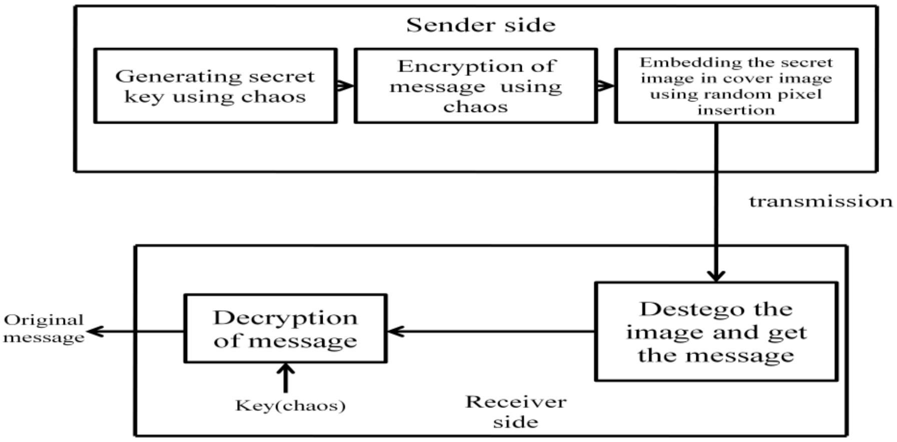
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014


Select chaotic map
Obtain bifurcation map
Identify chaotic region
Select a region from random region
Generate chaotic values of length equal to the no of pixels in the image
Rearrangethe chaotic values in increasing order
Rearrange the pixels as per the increasing order of chaotic values
Encrypted image

Figure(2) Block diagram of Encryption process

Second level of secrecy can be obtained in embedding these pixels in cover image. Redundant positions in the image can be selected to embed the pixels. For simplicity, we have embedded the scrambled pixels at periodic intervals.


Sender side
Generating secret key using chaos
Encryption of message using chaos
Embedding the secret image in cover image using random pixel insertion
transmission
Original message
Decryption of message
Destego the image and get the message
Key(chaos)
Receiver side

Figure(3) Block diagram of secret communication

At the receiving end, embedded pixels are collected back to get shuffled pixels of secret image. Same chaotic sequence is generated with identical constants and initial conditions are arranged in order to get back the correct positions of pixels. Thus original secret image can be recovered. The block diagram of the secrete communication is shown in figure (3).

IV. DEVELOPMENT ENVIRONMENT

Android is an open-source platform developed by Google and the Open Handset Alliance, using which interesting and powerful new applications can be quickly developed and distributed to many mobile device users. Some of Android-based devices are Motorola ANDROID, HTC DROID ERIS, and Google Nexus.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

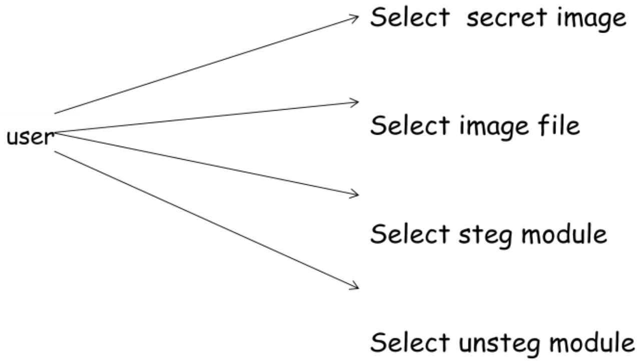
Vol. 2, Issue 7, July 2014

Android Development Tools (ADT) is a plug-in for the Eclipse IDE that is designed to give the users an integrated environment in which one can build Android applications. ADT extends the capabilities of Eclipse to let one quickly set up new Android projects, create an application UI, add components based on the Android Framework API and debug the applications using the Android SDK tools.

Android applications are written in Java, and then the compiled Java code is packaged into an Android package known as an .apk file. Bundling application data in this way allows applications to be easily distributed for installation on mobile devices. Indeed, the .apk file is the file that users are required to download and all the code in an .apk is essentially one application.

V. FRONT END DESIGN AND APPLICATION OUTPUT

For any application with android, front end design is very important. Here the user will have all choices to select the work to be done and images to be selected which they want to send secretly. Use case diagram for the application is shown in figure (4).



Figure(4) Use Case Diagram

Demonstration starts off with a login page with launcher icon for the application, where one has to enter the correct login password to begin the process. Start page is the next page encountered (Figure 5a). This page contains options like encrypt and decrypt.

On selecting option Encrypt, one enters into the next page.(Figure 5b). Options like Encrypt with chaos and stego are found in this page. Option encrypt with chaos deals with only encryption of secrete image and communicating it, while later deals with embedding encrypted image into a cover image and communicating. Once Encrypt with chaos is Chosen for image steganography, one needs to select a secret image in SD-card or camera. Chaos effect is applied on the secret image and the image obtained as a result is distorted or shuffled image. As seen (see Figure 6b) the pixels of the secret image are uniformly distributed once chaos pixel shuffling algorithm is applied. Chaotic values obtained will be seen in Log Cat.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

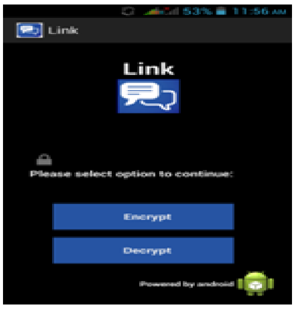
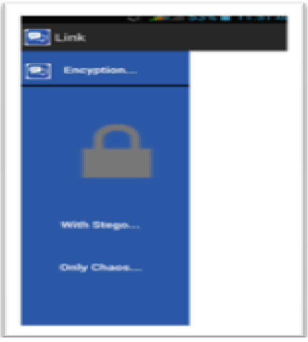
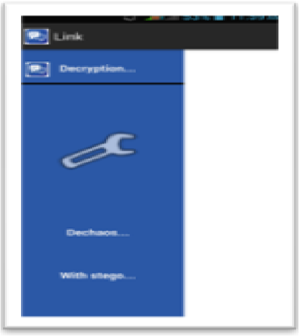


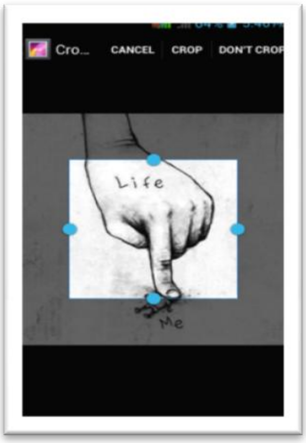
Fig 5 a. First page



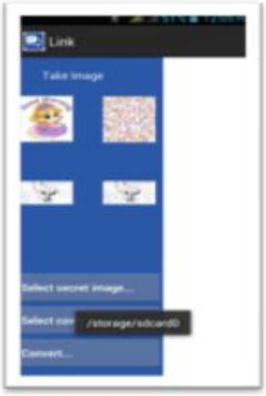
b. page for encryption



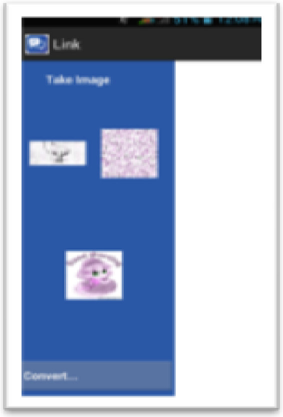
c. Page for decryption



e. Cropping cover image

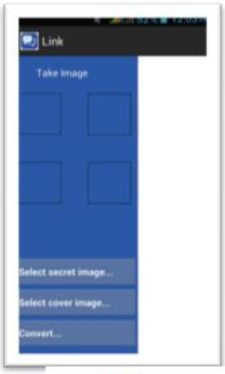


f. Stego image

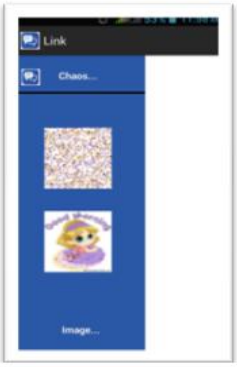


g. Extracting pixels and getting back original image

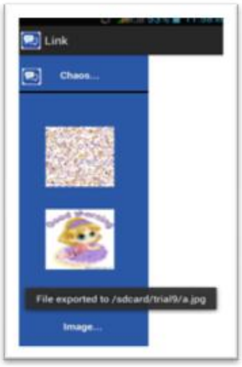
For steganography, Cover image is then selected and encrypted image is embedded within. At the receiving end, embedded pixels are collected back and decryption of shuffled image gives back the original image. Different pages of the application are shown in figure 5a to 5c,and 6a to 6g .



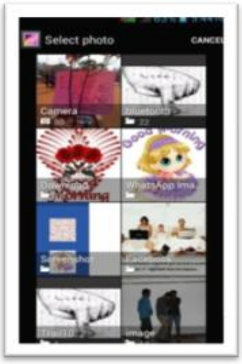
Fig(a)
Fig 6 a Front page



Fig(b)
b Encrypted image



Fig(c)
c. Saving to SD card



Fig(d)
d. Selection of image

An Android project contains all the files that comprise the source code for the Android app. The Android SDK tools make it easy to start a new Android project with a set of default project directories and files. Communication can be between any two android mobiles through mms, email or messengers like what'sapp

IV. PERFORMANCE ANALYSIS

A good encryption algorithm should be very much sensitive to the key. Sensitivity in key plays an important role because to some extent it eliminates the element of cryptanalysis. A slight variation in the key should result in totally different image in the rebuilding process at the destination. In this algorithm, the initial condition assumed to generate the chaotic map acts as the key. An effort to decrypt the encrypted image using another map or initial condition which differs by a very small value also will not give back the original image. Obtained results are shown in Figure 7.Figure 7(a) represents the original image, Figure 7(b) represents decrypted image using actual key and Figure 7(c) represents decrypted image with slightly different key i.e. initial condition. The above results are shown for Henon map with initial conditions 'a'=1.80000 (original key) and slightly different value 1.80001. From the obtained result it is clear that a slight variation, say 0.00001 results in totally different image.

The proposed algorithm will not cause statistically detectable artifacts, provided maximum payload which can be safely be hidden is selected. Here the pixel ratio used for secret and cover image is 1:6. If the secret image, which has to be hidden, has identical pixel values as that of the cover image, its performance will be better since there will be no difference in the intensity of the cover image even after applying steganography. Selected cover images which satisfy above conditions will yield better stego images

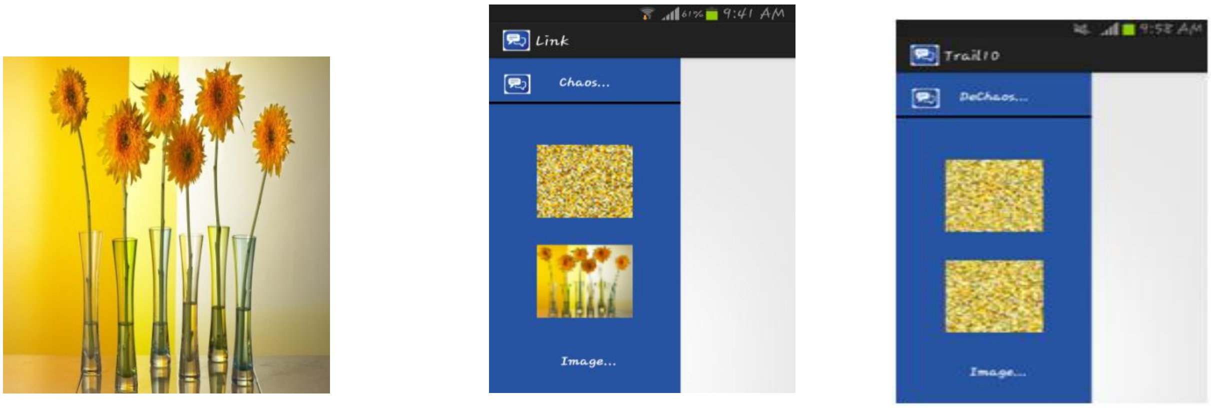


Figure 7a.Original image b. Decryption with original key a=1.80000 c. Decryption with a=1.80001

The peak signal-to-noise ratio, often abbreviated PSNR, is an engineering terminology that defines the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the representation of the signal. The PSNR is most often used as an important parameter to calibrate the quality of reconstruction of steganographic images. The signal in this case is the original image, and the noise is the error introduced by some steganography algorithm. It is most easily defined via the mean squared error (MSE) which for two m×n monochrome images I and K where one of the images is considered a noisy approximation of the other.

$$\mathrm{MSE} = \left(\frac{1}{\mathrm{MN}}\right) \sum_{\mathrm{i}=0}^{\mathrm{m}-1} \sum_{\mathrm{j}=0}^{\mathrm{n}-1} [\mathrm{I}(\mathrm{i},\mathrm{j}) - \mathrm{K}(\mathrm{i},\mathrm{j})]^2$$

$$PSNR = 10 \log_{10}(MAX/\sqrt{MSE})$$

MSE and PSNR for two images with the implemented algorithm are listed in table1 and values are satisfactory as for as the communication purpose is concerned.

Table 1:Performance analysis

IMAGE	MSE	PSNR
Doll image	1.4	23.3
Sunflower	0.89	24.3

VI. CONCLUSION AND FUTURE WORK

The paper describes about the application development for transmitting and receiving secret image through encryption and steganography using chaos in android platform. Key sensitivity is very high for this algorithm as unintended receiver will not be aware of the type of chaotic map used and initial conditions considered. MSE and PSNR are satisfactory for ordinary communication. The application developed can be easily used as multiple windows help in selecting required objects and achieving secret communication.

REFERENCES

1. Mintu Philip, Asha Das"Survey:Image Encryption using Chaotic Cryptography schemes" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011
2. Victor Grigoras1 , Carmen Grigoras "Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems" Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bucharest, Romania, October 16-18, 2006
3. Chen Wei-bin; Zhang Xin; "Image encryption algorithm based on Henon chaotic system" Image Analysis and Signal Processing, 2009. IASP 2009. International Conference, Publication Year: 2009, Page(s): 94 – 97.
4. Nien, H.H.; Huang, W.T.; Hung, C.M.; Chen, S.C.; Wu, S.Y.; Huang, C.K.; Hsu, Y.H.; "Hybrid image encryption using multi-chaos-system" Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on digital identifiers Publication Year: 2009 , Page(s): 1 – 5.
5. Xiaomin Wang; Jiashu Zhang; "An image scrambling encryption using chaos-controlled Poker shuffle operation" Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on Publication Year: 2008 , Page(s): 1 – 6.
6. Murali, K.; Haiyang Yu; Varadan, V.; Leung, H.; "Secure communication using a chaos based signal encryption scheme" Consumer Electronics, IEEE Transactions onVolume: 47, Issue: 4, Publication Year: 2001 , Page(s): 709 – 714.
7. Manjunath Prasad, K.L.Sudha," Chaos image encryption using pixel shuffling with Henon map" Elixir Comp. Sci. & Engg. Journal -38 (ISSN 2229-712X) 2011, 4496-4499
8. K.L. Sudha, Bhavana S, "Novel approach for Image steganography using Chaos" Serials publications- International Journal of Image Processing and Applications (IJIPA) (Jan-Jun. 2012) *ISSN: 0975-8178*
9. Mohammad Ali Bani Younes and Aman Jantan "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion" IJCSNS International Journal Computer Science and Network Security, VOL.8 No.6, June 2008
10. Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108
11. Venkatesh Asampelli, Patel ravi, bajirao Shinde Tushar Raut "Random LSB steganographic authentication Using eigen face recognisation technique for Mobile system" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 4, April 2014
12. Lubacz, J. Mazurczyk, W. Szczypiorski, K. "Vice over IP", Spectrum, IEEE, Volume: 47, Issue: 2 Publication Year: 2010 , Page(s): 42 – 47
13. http://developer.android.com/index.html
14. https://developer.android.com/training/basics/firstapp/index.html?hl=it

BIOGRAPHY

Savithri G is a B.E graduate in Computer Science and Engineering from K.S. School of Engineering and Management, Bangalore India. Her area of interest includes Information and Network Security, Android programming.

Dr.K.L.Sudha, presently working as professor in ECE department, Dayananda Sagar College of Engineering, Bangalore, India has 17 years of teaching experience in Engineering Colleges. She obtained her Bachelor's degree in electronics engineering from Mysore University and Masters from Bangalore University. She got Ph.D for her work on "Detection of FH CDMA signals in time varying channel" from Osmania University, Hyderabad. She has published more than 30 research papers in national / International journals and conferences. Her research interests are in Wireless communication, coding theory, image processing and chaotic theory.