Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.194 – 199

RESEARCH ARTICLE

Image Encryption Using Arnold's Cat Map and Logistic Map for Secure Transmission

Prerna Dureja[1], Bhawna Kochhar[2]

[1]Computer Science, PDMCE Bhadurgarh, India

[2]Computer Science, PDMCE Bhadurgarh, India

[1] Prernadureja13@gmail.com, [2] bhawna.kochhar9@gmail.com

Abstract-- Information security is primary requirement while information is transferring is public domain. To achieve this information security it is required to change the content format or send it in hidden form. Data encoding is provides the transformation of information in coded form so that the secure communication will be performed. But when there is the requirement to transfer some image data such as signatures, image password, biometric image etc. then there is the requirement to perform image encoding. In this present work, a two stage model is defined to achieve image encoding. In first stage of this model, the chaotic map is defined. This map is able to preserve the effective image information based on frequency analysis. The mathematical modeling is applied to generate chaotic map. Once the information is preserved, the encoding is performed using series of transformation operations. These operations include the phase transformation, radial transformation and bit adaptive transformation. The experimentation is here done on different image types including real time object images, biometric images and medical images. The analysis of work is done under MSE and PSNR values. The obtained result shows that the work has provided effective mechanism to provide image encoding.

Keywords- cryptography, Logistic Map, Arnold Cat Map, Chaotic Map, Security

I. INTRODUCTION

Data Encryption enables the information security while performing the private communication in public network. Cryptography is the encoding approach used to convert the raw information in encoded form so that the data integrity over the network is improved. Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form nonrecognizable by its attackers while stored and transmitted [1]. Today images are not only the way to represent or to provide the clear view of some object. But the image information can be critical enough to provide the authentication to some secure system. The image information security is one of the primary requirement while providing the information security over web. This information security mechanisms enables the data transmission over web in secure and effective way. Image cryptography actually deals in the image pixels under some defined mechanism. There are lots of approaches to used in image cryptography like chaining the pixel pattern, visual cryptography. There are number of sequence driven methods that enables the image cryptography. In this research, the main focus is to improve the transformation mechanism for image cryptography.

II. LITERATURE SURVEY

Lot of work is already done by different researchers to improve the information security under different media types and under different communication system. Some of the efforts of earlier researchers are discussed in this section.

In year 2012, Ohood S. Althobaiti, discuss the relationship between cryptography and mathematics in the context of Elliptic Curve (EC). Author presents the idea of biometric signature - a new method to combine biometrics with public key infrastructure (PKI), the security can be increased using the ECC in biometric signature creation, because the private and public keys are produced without saving and sending any secret information anywhere.

In Year 2012, Seny Kamara defined a work on Symmetric encryption using dynamic searchable technique. The presented approach allow a client to encrypt the data in such way the search can over the data can be performed over it. Author has defined SSE based scheme to satisfy the search condition. The work presented by the author actually extend the inverted index approach in different non-trivial ways and also introduce new technique to design the SSE.

Another work on visual information cryptography using the DH scheme was proposed by **Chao-Wen in year 2008**. Author presented an improved mechanism based deffie helman approach for visual cryptography approach. Author used a shared key mechanism using visual cryptography. Author used the half tone shadow images to show the work implementation. Author implemented the work using shared key and symmetric key approaches to achieve high level security [6].

A work on identity based cryptography was performed on symmetric cipher cryptography by **Joonsang Baek in year 2014.** In this paper, as contributions to this line of research, Author construct hybrid identity-based encryption schemes which produce compact cipher texts while providing both efficiency and strong security without resorting to the strong length preserving symmetric cipher.

Ueli Maurer in year 2011 performed a work on authentication based scheme using symmetric encryption. Author highlight two reasons for investigating nevertheless AtE as a general paradigm: First, this calls for a definition of confidentiality; what separates a confidential from a secure channel is its (potential) malleability. Author propose the first systematic analysis of malleability for symmetric encryption, which, in particular, allows us to state a generic condition on encryption schemes to be sufficient for AtE

In Year 2011, Parisa Kaghazgaran performed a work," Secure Two Party Comparison over Encrypted Data". Author defined an improve secure communication mechanism by using two party cryptography. In this approach, the parties included in the communication network provides the secure and reliable communication over the network by performing the key sharing. This key sharing algorithm is based on multiple comparison based cryptographic approach

III. METHODOLOGY

When we work on a network the security requirements of a user as well as a network increases. There are number of available ways over the network to achieve the information security. Image Cryptography is of the such way. But in last few years there are number of attacks that are implemented on watermarked images to reveal the actual information. In this present work, an effective image cryptography approach is presented using chaotic map and transformation approach.

III. I Signal Form Transformation

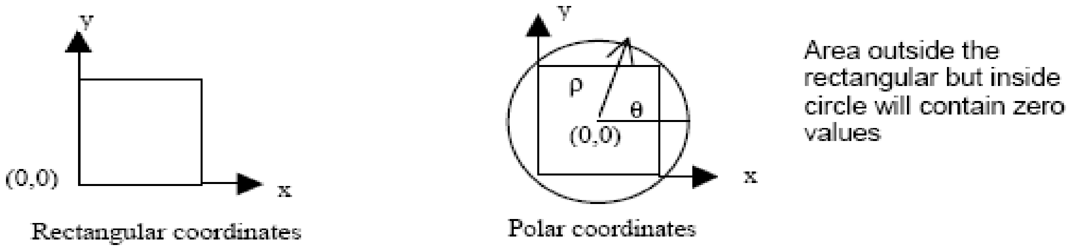
The image is transformed to signal form to process the encoding at earlier stage. The discrete Fourier transformation is the integrated matlab operation to apply this transformation. The expression form of this transformation is given as

$$\left|F\{I[m,n]\}\right| = \left|F[k,l]\right| = \left|\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I[m,n]\, e^{-j\left(2\pi/M\right)(km)}\, e^{-j\left(2\pi/N\right)(ln)}\right| \qquad (1)$$

DFT algorithm is here applied to improve the effectiveness of work. The phase transformation is applied to perform the transformation.

III. II Phase Transformation

Here FFT transformation is applied to achieve the coordinate independent log polar transformation applied on signal. The equation form of this transformation is shown in figure 1. To perform the FFT transformation, the log polar plane with coordinate system is given as under


y
(0,0)
x
y
ρ
θ
(0,0)
x
Area outside the rectangular but inside circle will contain zero values

Rectangular coordinates

Polar coordinates

Figure 1

This polar form of information is denied under equation parameter to provide the phase variation to achieve the image encoding. The pixel specific encoding provided by phase transformation.

III. III Radial Transformation

Once the phase transformation is done, the image is transformed to regular structured form and in this form, the image is divided in smaller blocks and on each block the radial transformation is here applied to achieve the block. The block sample generation and geometric sampling is here applied to generate the result image. The spatial variant geometry under sampling point specification is here done to generate the circle under log transformation. This transformation is applied respective to center and origin point specification so that the transformation to the circle points is done under specification of center. The transformation equation under distance vector is given by

$$I^*(p,\phi)=L\{I(x,y);(x0,y0)\}$$

Where

$$P= M \log(r+\alpha)$$

$$R=\sqrt{(x-x0)^2+(y-y0)^2}$$

$$\Phi = \tan^{-1}\left(\frac{y-y0}{x-x0}\right)$$

IV. SIMULATIONS

The interface is defined to process all the input and process stages in user interactive way. All the sub stages associated with this work are here presented in the form of separate stage.

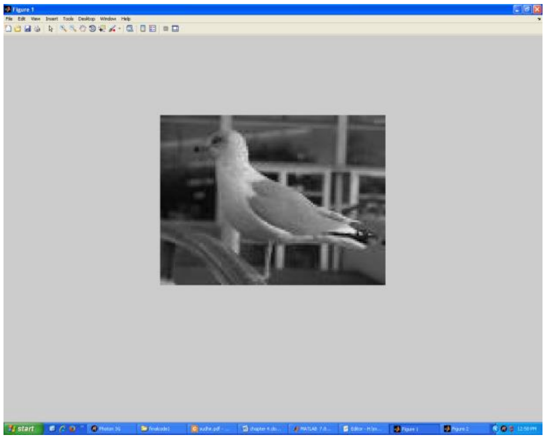


Figure 2

Here figure 2 is showing the input image taken on which the image cryptography will be applied.

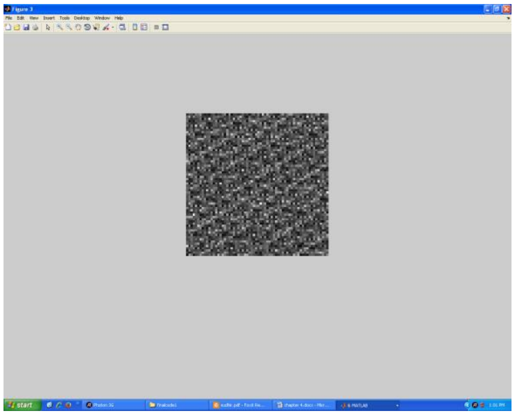


Figure 3

Here figure 3 is showing the results of encryption process defined as proposed model. The encoded image is shown hre in the figure.

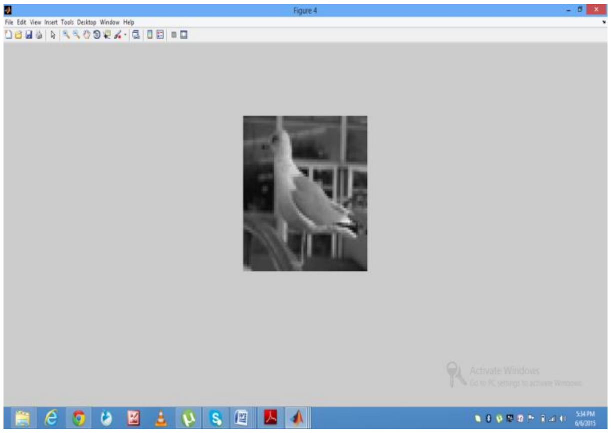


Figure 4

Here figure 4 is showing the results of decryption process defined as proposed model. The decoded image is shown here in the figure.

V. CONCLUSION

One of the major requirements for secure communication is to provide encoded form of communication. Image cryptography is used to achieve the encoding of image passwords or biometric images. In this present work, a two stage model is presented for image encoding. In first stage of this work, the chaotic map is defined for the input image. This map is able to preserve the effective image information. The chaotic map is generated to analyze the frequency domain and to provide the high intensity areas. The mathematical model is applied to generate chaotic map. In second stage of this model, the transformation is applied to perform encoding. In this work, phase transformation, radial transformation and bitwise transformations are applied to achieve image encoding. The result analysis is here done under MSE and PSNR parameters. The obtained experimentation results shows effective image encoding is performed.

VI. FUTURE WORK

In this present work, a two stage model is defined to perform the image encoding. The work can be improved in future under different aspects

- In this work, JPG image format is processed. In future some other image formats can be considered.
- In this work, no optimization to the approach is defined. In future some other optimization approach can be integrated.

REFERENCES

[1] Ercan Solak, Rhouma and Safya Belghith(2010),"Cryptanalysis of a multi-chaotic systems based image cryptosystem", Optics Communications 283 (2010) 232–236

[2] Ohood S. Althobaiti," The relationship between cryptography and mathematics in the context of Elliptic Curve (EC). ", International Journal of Emerging Technology and Advanced Engineering 2012, ISSN 2250-2459.

[3] Seny Kamara," Symmetric encryption using dynamic searchable technique ", International Journal of Scientific & Engineering Research 2012, ISSN 2229-5518.

[4] Parisa Kaghazgaran," The information security in case of involvement of more than one party in encryption process ", The International Arab Journal of Information Technology 2011.

[5] Trisha Chatterjee," Image the cryptographic algorithms for symmetric key cryptography ", International Journal of Advanced Research in Computer Science and Software Engineering 2013, ISSN: 2277 128X.

[6] Chao-Wen," visual information cryptography using the DH scheme ", International Journal for Science and Emerging Technologies with Latest Trends 2013, ISSN No. (Online):2250-3641, ISSN No. (Print): 2277-8136.

[7] Ueli Maurer, "2D image compression technique-A survey", International Journal of Scientific & Engineering Research 2011, ISSN 2229-5518.

[8] Ralf Kusters, "Implementation of Hybrid Dwt-Dct Algorithm for Image Compression: A Review", 2012, ISSN: 2249-3905.

[9] Nikita Bansal, "Image Compression Using Hybrid Transform Technique", Journal of Global Research in Computer Science 2013.

[10] Ahmad EL ALLAOUI, "Medical Image Segmentation By Markercontrolled Watershed And Mathematical Morphology", The International Journal of Multimedia & Its Applications 2012.