Image Encryption Using Chaotic Maps in Hybrid Domain

Dr.S.Ramahrishnan[1],B.Elakkiya[2]R.Geetha[3],P.Vasuki[4]
[1]Professor & head, [2, 3, 4] UG Scholars
Department of Information Technology,
Dr.Mahalingam College of Engineering and Technology

Received: 12-06-2014, **Revised:** 22-08-2014, **Accepted:** 26-09-2014, **Published online:** 02-11-2014

Abstract: **All image encryption systems are in the single domain. Hybrid domain (frequency and time domain) system is proposed to make the system more secured. We use the chaotic maps to generate pseudo random images. Since the chaotic maps have very good properties ,it will help us to encrypt the image in more secured manner. In our proposed system we employs two units: Transformation and substitution unit. We perform dft and dwt for the image. Transformation unit uses the tent map and substitution unit uses Bernoulli map**.

Keywords *Chaotic maps, tent map, bernoulli unit, Discrete Fourier transform, Discrete wavelet transform.*

I. Introduction

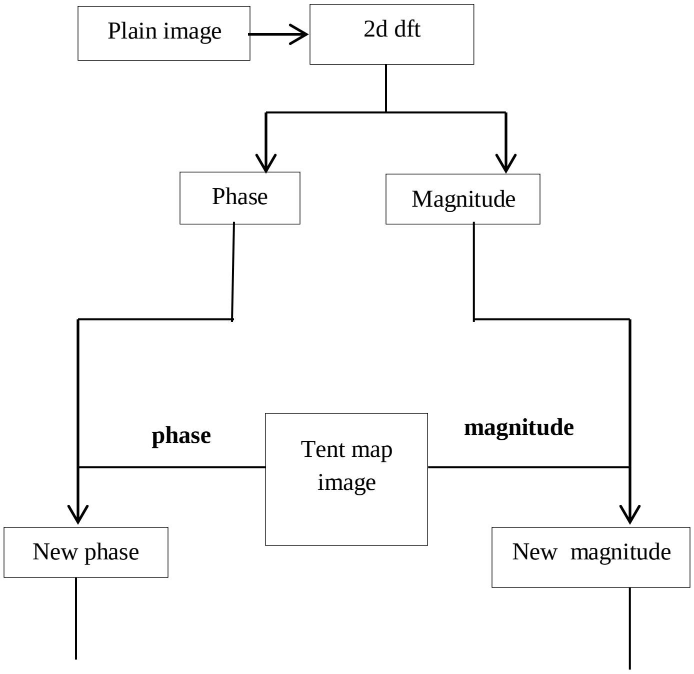
Encryption basically converts the information from its original form into some other form which is used to hides the information present in it. Encryption increases the data security in various transmission media.Image encryption is the process of converting the image into an unrecognizable format. Nowadays, the need for image encryption increases rapidly since it has application in the fields of medical image security, surveillance, videoconferencing, multimedia, military, etc., Traditional encryption systems like AES,DES,IDES,RSA, which are not well suited for image encryption . Because, in these encryption schemes, there exist an high correlation among the pixels, so it takes high computational time and power. Text encryption is different from image encryption. The image is less sensitive compared to the text data. While applying the traditional ciphers, due to the bulk capacity and high redundancy, it is easily attacked. For these reasons, to improve the security, flexibility and to reduce the computational time, chaotic image encryption system is introduced. Chaos has the properties like sensitivity to initial conditions and parameters ,as well as the mixing (ergodicity)and reproducible.Chaos Characteristics attracted many research people. Chaotic image encryption are resistance against attacks .so, it is a good measure for encrypting image. Chaotic maps are composed of parameters and are sensitive to tiny changes and possess random like behavior. Many researchers performed image encryption using the chaotic maps. Both two dimensional and three dimensional maps are employed. In [4],2-D baker map is further extended to 3-D map, to provide high security. Key in the image encryption process plays an important role for encryption and decryption. The proposed system is a private key encryption system, in which the same key is used for both encryption and decryption process.

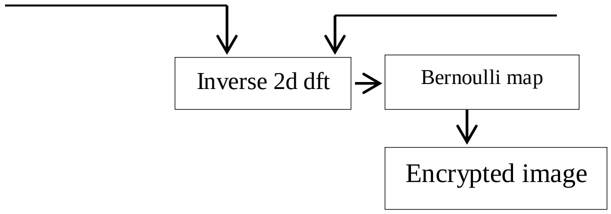
II. Related work

Image encryption is performed using frequency domain and time domain separately. Fridrich, J. (1997), Image encryption based on chaotic maps suggested a chaotic image encryption method in time domain. All the pixels in the image are moved using a 2D chaotic map and their values are altered sequentially. But image encryption performed using both time and frequency domain is more secured than the single domain system. Yaobinmao, guanrongchen, shiguolianA ,novel fast image encryption scheme based on 3D chaotic baker maps extended from 2D baker map with the has more intensive chaotic characters. In this image encryption scheme, an XOR plus modulo operation is Inserted to each pixel in between every two adjacent rounds of the map used .The experimental results show that this 3-D baker map is 2-3 times faster than the 2-D one, showing its great potential in real-time image encryption applications. N.K. Pareek, VinodPatidar , K.K. Sud , Image encryption using chaotic logistic map. An external secret key of 80-bit and two chaotic logistic maps are employed here. The initial conditions are derived for the two logistic maps using the selected external secret key by providing different weightage to its bits. ShahramEtemadi Borujeni1, and Mohammad Eshghi, Chaotic image encryption design using Tompkins-Paige algorithm.[3] Suggested image encryption using Tompkins-Paige algorithm in time domain . Tompkins-Paige algorithm is used to generate the target permutation matrix which is obtained from repetition of some simple permutations. Chaotic image encryption system using phase-magnitude transformation and pixel substitution[1], proposed the image encryption system in hybrid domain(frequency and time).It is more secured than the single domain system. In these Chaotic image encryption scheme, two maps are employed, which are used for generating pseudo random image

III. Existing system

i) Phase magnitude transformation unit:
2-D dft is performed on the plain image to covert the time domain into an frequency domain. The new phase and magnitude is generated.
ii) Tent map is used to generate the pseudo random image. phase and magnitude of this image is linearly combined with the phase and magnitude in the frequency domain and encrypted image -1 is obtained.
iii) Pixel substitution unit:
The pixels of the pseudo random image generated using the Bernoulli map is non-linearly combined with the pixels of the encrypted image-1. The new encrypted image -2 is obtained from it.Key1(128 bits) and key-2(320 bits) is used as initial value and parameter for the tent and Bernoulli map to generate pseudo random image.





IV. Proposed system

In our proposed system, we use two transformation, i.e.,DWT and DFT .Discrete wavelet transformation is used to work in time and frequency domain.Discrete Fourier Transform is used to work in frequency domain. Normally,Discrete Wavelet transformation computes for different segments of time domain signal at different frequencies.It does multiresolution analysis.

First, the plain Image is done level2 decomposition using DWT.The image is divided into seven subbands of 2,HL2,LH2,HH2,HL1,LH1,HH1.Apply DFT for the seven subbands each.We now have total of fourteen subbands phase and magnitude.

1) Transformation:

Chaotic tent map is used to do transposition of the image.

$$x(n+1) = r(0.5 - |x(n) - 0.5|)$$

Where x∈ (0,1).the control parameter p should be taken in range of (0,1) to keep the map chaotic.

We generate tent image using the above recursive formulae .DWT is applied to tent image and get seven subbands.now DFT is applied for each sub bands and get fourteen images. The New magnitude is calculated using the following equation

$$\left(LH_{Mag} + k * LH_{Mag(tent)}/(k+1)\right)$$

Where k=key.Calculate new phase and magnitude. Inverse 2D DFT is applied. Now we have new seven images.

2) Substitution:

The recursive equation of Bernoulli map is given below:

$x(k+1) = \big(b * x(k)\big) mod 1 \quad where\ x\ \in[0\ ,1]$

The control parameter of map should be in the range of[1,5] to keep the map chaotic. Chaotic Bernoulli map is used for substitution.DWT is applied for Bernoulli map image.These subbands are added to new subbands.Finally inverse DWT is done.Thus we get encrypted image. Thus chaotic image encryption is done in both the domains.Key is chosen from random number between one to seven and added to compute new phase and magnitude of subbands.

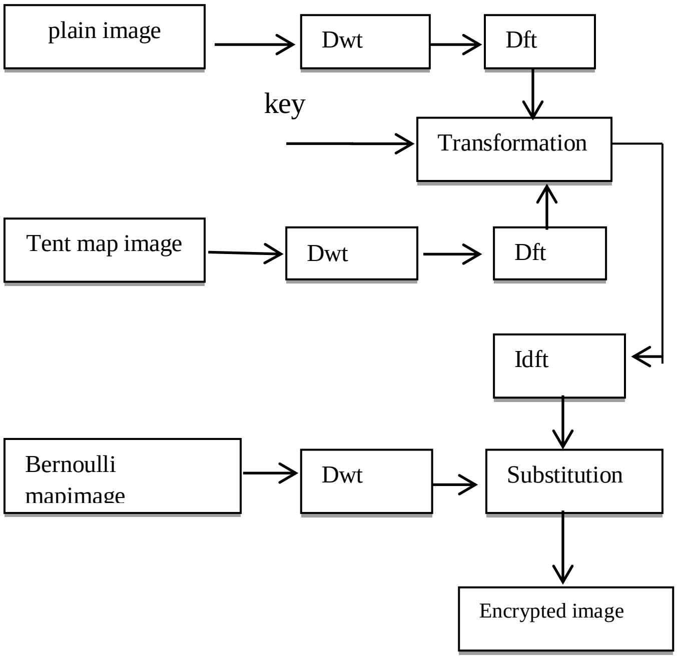


Fig2:Block Diagram of Proposed System

3)Simulation

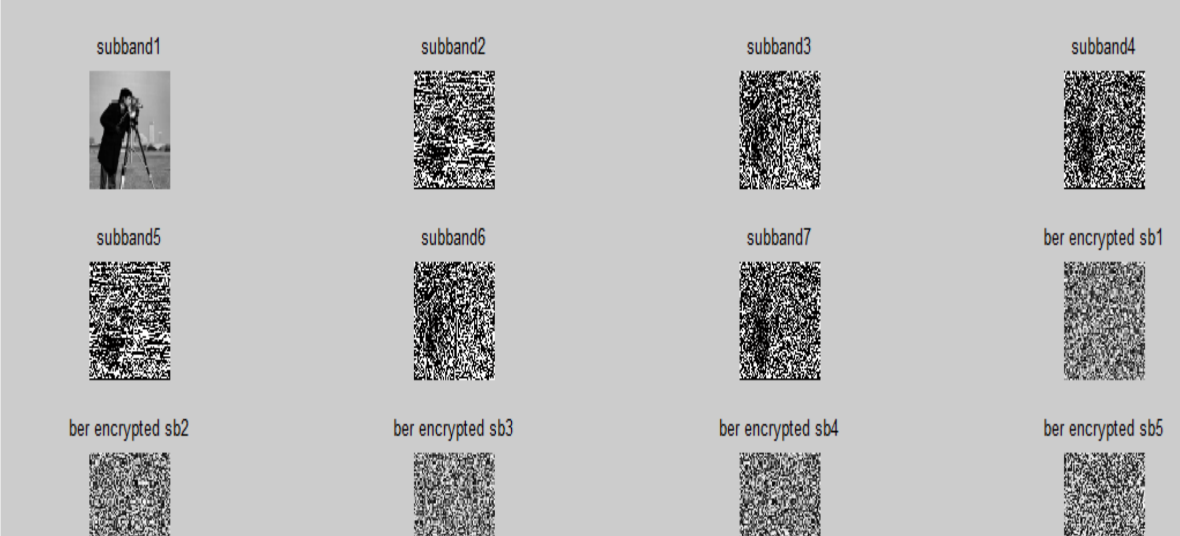
The system is simulated using MATLAB.

V. Security analysis

To secure images from statistical, brute force attacks we need a good encryption techniques. The proposed chaotic encryption system is analyzed by testing the performance of the system. In this section we discussed histogram analysis, correlation coefficient, mean square error, NPCR,UACI to prove that our proposed encryption system is more secure against most of the known attacks.

A.Histogram:

Histogram illustrates the distribution of pixels of an image. Histogram plays an important role in the security analysis.A good image encryption scheme should always generate a uniform histogram for the encrypted image. It is clear that the histograms of the encrypted images are fairly uniform and significantly different from the respective histograms of the original images and hence does not provide any clue



B.CorrelationCoeffic

I. ient:

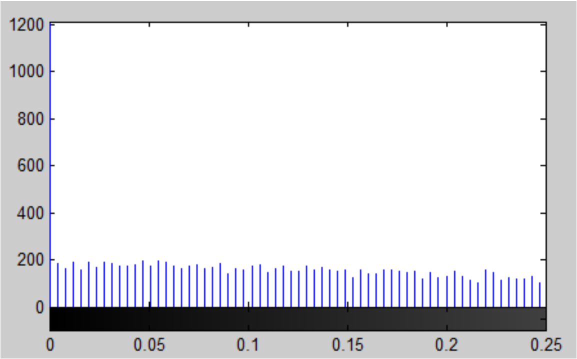


Fig3:histogram of encrypted image

B)Correlation Coefficient

The correlation coefficient is used to evaluate ,quality of theproposed encryption system. Correlation coefficient should be low for secure the encryption system against the statistical attacks. It is calculated between two vertically, horizontally, diagonally adjacent pixels of an encrypted images. The following equations are used to calculate the correlation coefficient $C_{(a,b)}$,

$$C(a,b) = \frac{COV(a,b)}{\sqrt{R(a).R(b)}}$$

$$R(a) = \frac{1}{M}\sum_{i=1}^{N}\left(ai - \frac{1}{M}\sum_{i=1}^{N} aj\right)^2$$

$$COV(a,b) = \frac{1}{M}\sum_{i=1}^{N}\big(ai - E(a)\big)\big(bi - E(b)\big)$$

Where a and b are gray scale values of two adjacent pixels in the image and E represents expectation operator.The correlation coefficient of encrypted image is -0.0240.

C. Mean Square Error:

The mean square error refers the difference between encrypted image and the plain images.The MSE value should be larger for the better encryption security. The MSE is defined by

MSE=$\frac{1}{S\times S}\sum\sum(Xij - Yij)^2$

S represents size of the image and the parameters of the gray scale values of pixels in plain image ,encrypted images are denoted by x_{ij},y_{ij}respectively.MSE of encrypted image is 17952.

D.NPCR:

The Number of Pixels Change Rate(NPCR) measure the percentage of different pixel values between two images.The two encrypted images are taken and whose corresponding images should have only one pixel difference.

$$\text{NPCR} = \sum_{i,j} \frac{C(i,j)}{xy} \times 100\%$$

Where x and y are the width and height of the encrypted imageNPCR value of the encrypted image is 100.00.

E.UACI:

The Unified Average Changing Intensity(UACI) refers average intensity in a gray level of the corresponding pixels of an encrypted images.

$$UACI = \sum_{i,j} \frac{C1(i,j) - C2(i,j)}{F.T} \times 100\%$$

T refers total number of pixels in the encrypted image.F refers largest supported pixel which is compatible with the encrypted image.The encrypted image value for UACI is 46.88

References

1. ShahramEtemadiBorujeni ,& Mohammad Eshghi(2013) .Chaotic image encryption system using phase-magnitudetransformation and pixel substitution,TelecommunSyst (2013) 52:525–537DOI 10.1007/s11235-011-9458-8.
2. Pareek, N. K. (2006). Image encryption using chaotic logistic map.*Image and Vision Computing*, *24*, 926–934.
3. Borujeni, S. E., &Eshghi, M. (2009). Chaotic image encryptiondesign using Tompkins-Paige algorithm.Journal of Mathematical Problems in Engineering, 2009, Modeling experimental nonlinear dynamics and chaotic scenarios, p. 22. oi:10.1155/2009/762652.
4. Mao, Y. B., Chen, G. R., &Lian, S. G. (2004).A novel fast imageencryptionscheme based on 3D chaotic baker maps.*International Journal of Bifurcation and Chaos*.
5. Mitra, Y. V., Rao, S., &Prasanna, S. R. M. (2006). A new image encryption approach using combinational permutation techniques.*International Journal of Computer Science*, *1*, 127–131.
6. Rijndael (2001). Announcing the ADVANCED ENCRYPTIONSTANDARD (AES), *Federal Information Processing StandardsPublication 197*.
7. Gonzalez, A.,Woods, A., &Eddins, A. (2004). *Digital image processing using MATLAB.*
8. TommasoAddabbo, IEEE, Massimo Alioto, Ada Fort, SantinaRocchi, and alerioVignoli, (2006).The Digital Tent Map: Performance Analysis and Optimized Design as a Low-Complexity Source of Pseudorandom Bits .IEEE Transactions on Instrumentation and Measurement, vol. 55, no. 5
9. .XunYi(2005) Hash Function Based on Chaotic Tent Maps. IEEE Transactions on Circuits and Systems—ii: express briefs, vol. 52, no. 6
10. .http://www.mathworks.com
11. Kamlesh Gupta1, Sanjay Silakari,(2011). New Approach for Fast Color Image Encryption Using Chaotic Map. Journal of Information Security, 2011, 2, 139-150
12. FethiBelkhouche, UvaisQidwai, Ibrahim Gokcen, Dale Joachim.(2004). Binary Image Transformation Using Two-Dimensional Chaotic Maps .0-7695-2128-2/04 $20.00 © 2004 IEEE.