BLOCK IMAGE ENCRYPTION USING WAVELET

Dr.S.Ramakrishnan[1], M.Sasipriya[2], R.Saranya[3] , M.Priyanka[4]

[1]Dr.S.Ramakrishnan,Professor,
[2]M.Sasipriya, Student, [3]R.Saranya, Student, [4]M.Priyanka, Student

---***---

Abstract - *Image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Images are also processed as three-dimensional signals where the third-dimension being time or the z-axis. The two-dimensional Discrete Wavelet Transform (2D-DWT) is now a key operation in image processing. Discrete wavelet transform (DWT) is a wavelet transform for which the wavelets are discretely sampled. Compared with other wavelet transforms, a key advantage is that it has over Fourier transforms is temporal resolution that it captures information of both frequency and location. The disadvantage of DWT is that it requires more processing power. Finally calculate the number of changing pixel rate (NPCR) and the unified averaged Changed intensity (UACI) two most common quantities used to evaluate the strength of image encryption algorithms/ciphers. This technique provides high level authentication and security.*

***Key Words*: 1.Wavelet transform,2. NPCR ,3.UACI**

1. INTRODUCTION

Image Processing is processing of images using mathematical operations by using any form of signal processing for which the input is an image, a series of images, or a video, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Images are also processed as three-dimensional signals where the third-dimension being time or the z-axis. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging.

Closely related to image processing are computer graphics and computer vision. In computer graphics, images are manually made from physical models of objects, environments, and lighting, instead of from natural scenes, as in most animated movies. Computer vision, on the other hand, is often considered high-level image processing out of which a machine/computer/software intends to decipher the physical contents of an image or a sequence of images The two-dimensional Discrete Wavelet Transform (2D-DWT) is nowadays established as a key operation in image processing.

The paper is structured as follows. Section II analyzes of techniques used. Section III discusses the proposed system of our project and its module description. Section IV provides the results and discussions.

2. TECHNIQUES USED

A. Logistic map

In mathematics chaotic map can be defined as a function that exhibits chaotic behavior. Both continuous and discrete chaotic maps are available. In this work discrete map is used, this kind of maps usually takes the form of iterated functions. In this work logistic map is used. The logistic map is a simple one dimensional map and is given as,

$$x_{n+1} = rx_n(1-x_n)$$

Logistic map is a polynomial mapping of degree. In above Equation X_n € [0, 1] and is known as the phase space of the logistic map, r is the control parameter that controls the behavior of the map.

- With r between 0 to 1 the map is independent of the initial condition.
- For r between 1 to 2 the trajectory will quickly reach the value, map is independent of the initial condition.
- For r between 2 to 3 the trajectory will reach the value in as specific manner that is it will revolve around the value for some time to reach the value.

- With r between 3 to 3.45 for almost all the initial conditions the population will oscillate between two values and these values are depends on the value of b.
- At r approximately 3.57 is the onset of chaos, at the end of the period-doubling cascade. From almost all initial conditions we can no longer see any oscillations of finite period. Slight variations in the initial population yield dramatically different results over time, Frank et al (2001) stated prime characteristic of chaos.

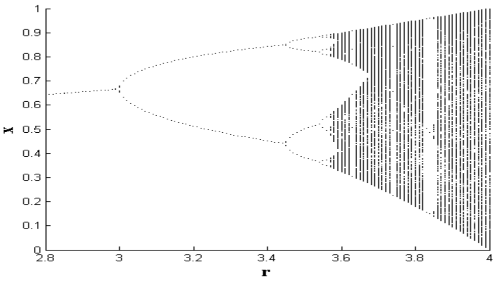


Figure 1.1 Bifurcation diagram of logistic map

- Beyond r = 4, the values eventually leave the interval [0, 1] and diverge for almost all initial values.

- Figure 1.1 summarizes the above points and the horizontal axis shows the values of the parameter r while the vertical axis shows the values of x. From Figure 1.1 it is clear that for the values above r = 3.82 the map exhibits the chaotic behavior proposed by Parker et al (1995). The map used in this work is a discrete one, it is in the form of iterated function. This map is used because of its easy computation and greater complexity.

B. Wavelet transform

A wavelet is a mathematical function used to divide a given function or continuous time signal into different scale components. Usually one can assign a frequency range to each scale component. Then it can be studied with a resolution that matches its scale. A wavelet transform is represented by wavelets function. The wavelets are scaled and translated copy of a finite length or fast decaying oscillating waveform (known as the "mother wavelet"). Advantages over traditional Fourier transforms for representing functions that are discontinuities and sharp peaks, and for accurately deconstructing and reconstructing finite, non-periodic or non-stationary signals.

Wavelet transforms are classified into discrete wavelet transforms (DWTs) and continuous wavelet transforms (CWTs). DWTs use a specific subset of scale and translation values or representation grid. Applications of wavelet transform are transform data, and then encode the transformed data, resulting in effective compression and for communication applications.

C. Discrete wavelet transform

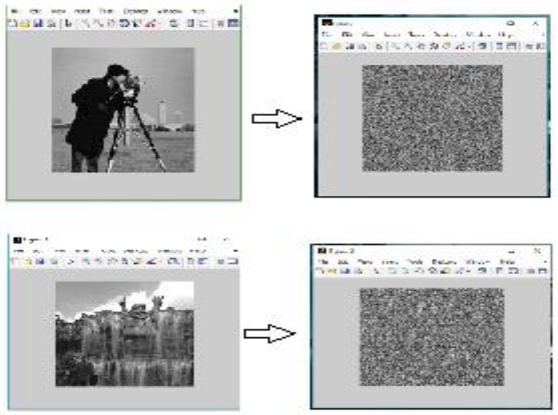
DWT is any wavelet transform for which the wavelets are discretely sampled. Compared with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: that it captures information of both frequency and location. Applications for discrete wavelet transform are signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression, Practical applications are also found in signal processing of accelerations for gait analysis and in digital communications.

3. IMPLEMENTATION

Several techniques were used for image encryption. In the implementation part we use block image for encryption. A plain image is taken and made into blocks. The chaotic map will be generated for the random number generation. In that we use Logistic Map that exhibits the chaotic behavior. Along with the plain image a key image also called cover image is taken and the same chaotic function is repeated for it. The sender will encrypt the image and Decrypted by receiver where the Key has been shared among the users. This process is done to make the secure transmission of data. We use wavelet because Wavelets can be combined, using a "reverse, shift, multiply and integrate" technique called convolution, with portions of a known signal to extract information from the unknown signal. Along with this implementation we use DWT for the image encryption. The tool used is MATLAB R2013a[8].

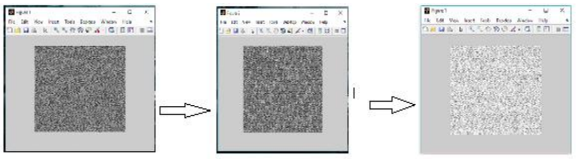
A. original and cover image permutation

The camera man image is taken as an original image for our process. Size of the image will be 256*256.A cover image is taken and is permuted.



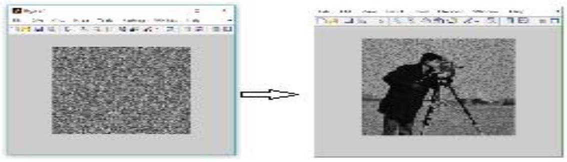
B. Encryption

In this process the original image is in the form of two dimensional matrix. The two dimensional matrix is then converted into one dimensional matrix. Then the chaotic map will be generated for the random number generation. In that we use Logistic Map that exhibits the chaotic behaviour.



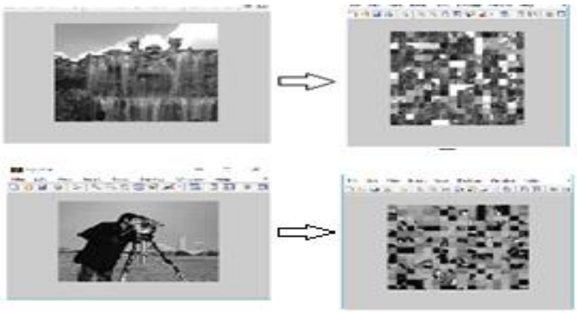
C. Decryption

In this implementation of image encryption algorithm is proposed based on combination of pixel shuffling and chaotic maps. Shuffling is used to expand diffusion in the image and dissipate the high correlation among image pixels. Due to sensitivity to initial conditions, chaotic maps have a good potential for designing dynamic permutation map. Reverse of the process is done in order to obtain the original image.



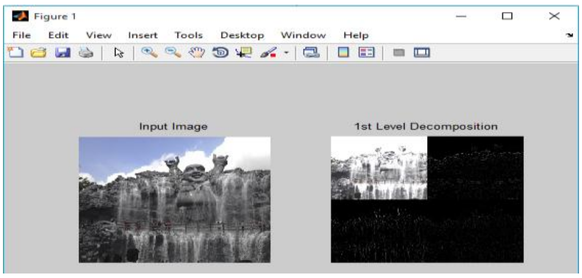
D. Block based image encryption

In block based image encryption, the original image is made into sub blocks i.e. *16*16.* The original image is of 256*256 and is made into blocks where these blocks are then shuffled randomly. This random shuffling will provide the confusion for the attacker. Similarly a cover image for it is also shuffled as same as the original image.



E. First level of decomposition

The original image is first segmented into four sub bands of (LL, LH, HL, HH) by applying integer wavelet transform



4. RESULTS AND DISCUSSIONS

The plain image and changed pixels is taken to calculate the NPCR and UACI. C_1(i,j) is the encrypted plain image and C_2(i.j) is the changed pixel key image.

NPCR AND UACI

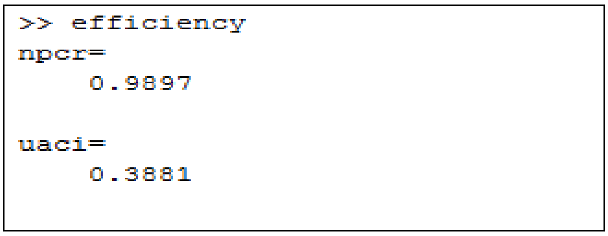
The number of changing pixel rate **(NPCR)** and the unified averaged changed intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers.

The NPCR and UACI is to test the number of changing pixels and the number of averaged changed intensity between cipher text images, while the difference between plaintext images is a single pixel. Then these two tests are easy to calculate. Example, the upper-bound of the NPCR score is 100%, and it is believed that the NPCR score of a secure cipher should be very close to this upper-bound.

The attacker have a slight change that can modify one pixel of the plain image to find some meaningful relationships between the plain image and the encrypted. If a minor change in the plain image makes a significant change in the cipher image, this shows that the encryption scheme resists differential attacks more efficiently. To test the influence of only one pixel change in the plain image over the whole encrypted image, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI),

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UCAI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right] \times 100\%$$



```
>> efficiency
npcr=
     0.9897

uaci=
     0.3881
```

5. CONCLUSIONS

Image encryption based on gray scale images has been implemented. Applying DWT for the image, the sub bands are generated and was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted and decrypted.

Performance was evaluated using statistical parameters such as number of changing pixel rate **(NPCR)** and the unified averaged changed intensity (UACI). These values are calculated to evaluate the strength of image encryption algorithms/ciphers. And to compare whether the performance is good enough. Future enhancement would be applying this technique in order to improve the high level security in image transmission on internet and also improve the computational ability. Hence it gives good imperceptibility and security.

ACKNOWLEDGEMENT

The authors wish to express their gratitude to the anonymous reviewers for their valuable comments and suggestions to improve the quality and paper.

REFERENCES

[1] Z.Liu,M.Gong,Y.Dou,F.Liu,S.Lin,M.AshfaqAhmad,J.Daia, S.Liu,DoubleimageencryptionbyusingArnoldtransformanc discretefractionalangulartransform,Opt.LasersEng.50(2012)248–255.

[2]Liu, Z., Guo, Q., Xu, L., Muhammad, A.A., Liu, S., " Double image encryption by using iterative random binary encoding in gyrator domains", Optics Express 18(11), 12033–12043, 2010.

[3]P.Moulin,Theroleofinformationtheoryinwatermarkinganditsapplicationtoimage watermarking,SignalProcess.81(6) (2001)1121–1139.

[4]ChenGR,MaoYB,ChuiCK.Asymmetricimageencryptionbasedon3Dchaoticcatmaps.ChaosSolitonsFractals2004;21 (3):749–61.

[5]GuanZH,HuangFJ,GuanWJ.Chaosbasedencryptionalgorithm.PhysLettA 2005; 346(1–3):153–7

[6] Cahit C, Ercan S. Cryptanalysis of a chaos-based image encryption algorithm. PhysLettA2009;373(15):1357–60.

[7] Wang K, PeiWJ, LiuHZ, HeZY. On the security of 3D catmap based symmetric image encryption scheme. PhysLettA2005;343(6):432–9.