High Secured Image Encryption using Hyper Chaotic and DNA

Nagireddi Divya[1], K. Suresh[2]

[1]*M.Tech Scholar, Dept. of ECE, Chaitanya Engineering College, Komadhi, Visakhapatnam, Andhra Pradesh, India.*

[2]*Associate Professor, Dept. of ECE, Chaitanya Engineering College, Komadhi, Visakhapatnam, Andhra Pradesh, India.*

Abstract- A new color image encryption algorithm based on DNA (Deoxyribonucleic acid) sequence addition operation is presented. Firstly, three DNA sequence matrices are obtained by encoding the original color image which can be converted into three matrices *R*, *G* and *B*. Secondly, we use the chaotic sequences generated by Chen's hyper-chaotic maps to scramble the locations of elements from three DNA sequence matrices, and then divide three DNA sequence matrices into some equal blocks respectively. Thirdly, we add these blocks by using DNA sequence addition operation and Chen's hyper-chaotic maps. At last, by decoding the DNA sequence matrices and recombining the three channels *R*, *G* and *B*, we get the encrypted color image. The simulation results and security analysis show that our algorithm not only has good encryption effect, but also has the ability of resisting exhaustive attack, statistical attack and differential attack.

I. INTRODUCTION

Now-a-days data transmission is prominent in any sort of communication and the importance of a particular type of data can vary from lower to higher level. In the present age of technology, cybercrime is quite common and the security of data may easily be compromised. In order to counter the unauthorised access and data theft, a suitable data protection technique should be developed. Data encryption is one of the important data protection techniques which widely used in information security. Image data encryption has gained popularity since any type of data can be represented in the form of an image. Conventional cryptographic algorithms like AES, DES, may be quite successful in encrypting raw data of small size but cannot provide good results in encryption of the digital images. These algorithms are unable to exploit the correlation among the adjacent pixels, which is an inherent property of an image. Rigorous research is going on the techniques of encrypting an image. Any standard encryption algorithm performs basic three operations: pixel permutation, diffusion and confusion. However, as the time passed by, these encryption algorithms started to fall prey to certain stringent security test. Desirable randomness in the generated sequence could not be obtained from these algorithms. Hence non-linear science started to gain popularity. Chaos theory introduced by Edward Lorenz became the building block of chaos based image encryption techniques. A certain set of deterministic equations composed of a number of state variables and fixed parameters may result in a sequence which is deterministic but unpredictable when iterated for a number of times. The generated sequence exhibits an inherent behavior of randomness and this property is widely exploited in designing the chaos based cryptosystems. In the literature of chaos-based cryptography, generally, four types of chaotic systems (discrete time, continuous time, time delay and hyperchaotic) used as entropy sources in an encryption algorithm. The role of the chaotic system in encryption algorithm is to generate the chaotic key sequence for pixel permutation and confusion. A few examples of chaos based cryptosystems along with their merits and demerits are discussed in the next section.

II. LITERATURE SURVEY

Qinglong Huang *et al.* [1], "Secure Image Encryption Technique Based on Multiple Fresnel Diffraction Transforms", (2006) proposed a new secure image encryption algorithm based on the multiple Fresnel diffraction transforms (MFDTs). In that algorithm the MFDTs depend strongly on the diffraction distances, the decryption can proceed when the all keys are correct, and the algorithm is robust to the attacks, such as JPEG lossy compressing, cropping, superposing noise, and resampling from the screen copy. There is no simple "one-to-one" relationship between the plain text and cipher text in the MFDTs, it is extremely difficult to decrypt the keys with the exhaust research method, the optical scanning method, and the known-plaintext phase retrieval algorithm. Concluded that, the encryption algorithm has a higher level of security.

Yi Xin*et al.*, [2], "Image Encryption Based on a Novel Reality-Preserving Fractional Fourier Transform", (2006) proposed a novel method of digital image encryption. Image encryption and decryption were performed based on the continuously increasing decorrelation property and the real-valued ness of the reality-preserving fractional Fourier transform. The input and encrypted data are respectively in the spatial domain and the reality preserving fractional Fourier transformed domain determined by encryption keys. The encrypted image is real-valued, so it's convenient for display and storage. The parameters of the reality-preserving fractional Fourier transform enhance the space of keys. As a method of encryption, it won't bring data expanding, and is

sensitive to parameters, with considerable robustness, security, and feasible.

Hone-Ene Hwang, *et al.* [3], "A Novel Wavelet Transform Algorithm for Image Encryption", (2006) Proposed A high efficiency digital security system based on the discrete chirp parent wavelet transform (DCPWT). And said that algorithm is outstanding than other precedent schemes on two aspects: no iterations are needed and the image is recovered exactly (no information is lost). From results, concluded that high security can be assured with four sensitive parameters (keys) and it is important that this scheme can be used on high speed digital communication line.

Changjiang Zhang *et al.* [4], "Digital Image Watermarking Algorithm with Double Encryption by Arnold Transform and Logistic", (2008) proposed an algorithm for watermark inserting and detecting algorithm based on stationary wavelet transform in this method firstly the digital watermarking was transformed randomly (Arnold transformation), then encrypted by logistic. The encrypted watermarking was transformed to one-dimensional row vector, and the pixel value was sorted. The coefficient of one-dimensional of primitive image of stationary wavelet transformation was sorted too, then inserted sorted watermarking to the sorted low frequency, and turned it to two dimension data. Then the image is reconstructed with coefficients of high-frequency. The process of watermarking inserted is the inversion of the process of watermarking embedded. Finally withdraw the watermarking and obtained the primitive watermarking after the anti-Arnold transformation. This algorithm chose the appropriate position to insert the watermarking. From experimental results concluded that this algorithm not only enables the watermarking to have the very good invisibility, but also makes the watermarking have very strong robustness to the general image attacks, such as noise, filter, rotation, compression etc.

Zheng Wei *et al.* [5], "Image Data Encryption and Hiding Based on Wavelet Packet Transform and Bit Planes decomposition", (2008) proposed a novel approach to encrypting and hiding gray scale images with wavelet packet transform and bit planes decomposition. The proposed strategy can be applied not only to encryption and hiding of a single image, but also to multi-frame images. Wavelet packet transform is used to decompose a carrier image into sixteen sub-band images, and eight high frequency and high entropy value of sub-images would be selected as carrier of a secret image from them. A chaotic sequence is employed to encrypt a secret image. And then the encrypted image is decomposed into eight bit planes. After impact factors of the bit planes are selected, the bit planes would separately be superimposed on the eight sub-band images in accordance with entropy values of the sub-images and information amount of the bit planes. Finally, the carrier image embedded the secret image is reconstructed using wavelet packet inverse transform. He concluded that it show the approach is able to not only maintain fidelity of the carrier image, but also ensure security and safety of the secret image.

Hiroyuki Yoshimura*et al.* [6], "New encryption method of 2D image by use of the fractional Fourier transform", (2008) proposed an algorithm for secure transmission of image information. It is very significant especially with the development in the internet. Encryption method of 2D image by use of the fractional Fourier transform (FRT) which is the generalization of the conventional Fourier transform (FT). Specifically the FRT with different order of the FT is conducted to the gray scale distribution in each line of the original image. Proposed encryption method is analyzed using parameter cross-correlation between the original image and the encrypted image. Chun-jiang pang, in the paper, "An image encryption algorithm based on discrete wavelet transform and two dimension cat mapping" (2009) proposed an algorithm for image encryption, for the generation of two value sequences by separating the two-dimensional cat mapping sequence, according to the distribution of this two value sequence, establish exclusive corresponding relationships between the two-dimensional cat mapping chaos sequence and the discrete wavelet transformation coefficient matrix. The value of the discrete wavelet transformation coefficient matrix was encrypted and the scrambled by adjusting chaos sequence. Concluded that, this algorithm can overcome the flaw of lower-dimensional chaos dynamics system easy to attack, and has the characteristics of highly secrecy, simple key, precise uniformity between restructuring image and original image. It has one of the additional feature that it can withstand the noise effect from the transmission process.

Hui Zhao*et al.* [7], "Image Encryption Based on Random Fractional Discrete Cosine and Sine Transforms", (2009) proposed an algorithm for the image encryption using a new fractionalization of discrete cosine and sine transforms of types I, IV, V and VIII. The fractional discrete cosine and sine transforms with four random parameters are defined, to which we refer as random fractional discrete cosine and sine transforms. Algorithm based on random fractional discrete cosine or sine transform and random phase encoding technique is proposed. Analysis of the quality of encryption is done using the mean square error v/s change of order of transform.

Cheng-Hung Chuang *et al.* [8], "Adaptive Steganography-based Optical Color Image Cryptosystems",(2009), proposed an image encryption and decryption algorithm based on an optical cryptosystem with adaptive steganography for color image. The optical cryptosystem employs a double random phase encoding algorithm to encrypt and decrypt color images. The color image is first separated into three channels: red, green, and blue. Each channel is encrypted by two random phase masks generated from session keys. For higher security, an asymmetric method is applied

to cipher these session keys. The ciphered data produced by the asymmetric method is then embedded into the encrypted color image by a content dependent and low distortion data embedding technique. The key delivery is accomplished by hiding ciphered data into the encrypted color image with a specific hiding sequence generated by the zero-LSB sorting technique. From experimental results concluded that the proposed adaptive steganography-based cryptosystem has a good performance when it is applied to color images.

Nanrun Zhou *et al.* [9], "Optical image encryption scheme based on multiple parameter random fractional Fourier transform", (2009) proposed a method for the image encryption with multiple parameter random fractional Fourier transform (MPRFrFT). By randomizing the transform kernel of the basic function from multiple-parameter fractional Fourier transform, MPRFrFT inherits the excellent mathematical properties of the fractional Fourier transform. The method of MPRFrFT image encryption algorithm includes five parameters, i.e., keys. An optical realization for MPRFrFT image encryption is provided. Concluded with the results the feasibility and superior robustness to blind decryption of the method.

Lin Zhang *et al.* [10], "Image Encryption with Discrete Fractional Cosine Transform and Chaos", (2009) proposed image encryption algorithm with discrete factional cosine transform (DFrCT) and chaos. DFrCT holds the particular properties which the conventional discrete cosine transform (DCT) hasn't, that is its fraction. Chaos functions have extreme sensitivity to the initial conditions. Logistic map is a simple equation of chaos functions. XOR is first operated between the original image and logistic map. Then the chaotic image is transformed with DFrCT two times using different keys successively by rows and by columns. Based on this method, the image can encrypted effectively, also, the transmission of the encrypted image with DFrCT and chaos is faster than with fractional Fourier transform (DFrFT) and chaos. Analysis of the encryption algorithm is done using the mean square error (MSE) between the original images and the decrypted images.

Jun LANG *et al.* [11], "The Generalized Weighted Fractional Fourier Transform and Its Application to Image Encryption", (2009) proposed a method for the image encryption using Shih's weighted fractional Fourier transform is generalized to contain two 4D vector parameters (M,N) ∈Z4,which is denoted by Generalized Weighted Fractional Fourier Transform (GWFRFT). GWFRFT is shown to possess all of the desired properties for Shih's FRFT. In fact, the GWFRFT will reduce to Shih's FRFT when both M,N are zero vectors. The eigenvalue relationships between GWFRFT and two original FRFT were used. Its multiple-parameter feature and the double random phase encoding in the GWFRFT domain for digital image encryption. Concluded that the method of encryption in the GWFRFT domain can enhances data security.

III. EXISTING SYSTEM

To gain a consistent method for encryption has been always in need even all over the past. Several encryption applications are in an assortment from defense and intelligences utilize in profitable undertakings on daily basis. An expertise has enhanced to take into account simpler and improved encryption and transmission, hence it has also permitted the development in interception and cryptanalysis. Codes have been turn out to be further progressive, developing from simple character replacement ciphers to today's algorithm of large pseudo-primes, exponents, and particular consistency.

In any case the idea has stayed basic; it is anticipated to have the capacity to send data starting with one point then onto the next without any one having the capacity to comprehend it in the mid. The appearance of the web has made security of information and assurance of protection a significant reason for concern toward anybody. The profoundly eccentric and irregular look nature of chaotic signals is the most tempting feature of deterministic chaotic system that may prompt to as novel applications. With the quick advancement of the computer innovation and data processing technology, the issue of data security is constantly more imperative. Data hiding away is normally used to secure the imperative data from unveiling when it is transmitting over an uncertain channel.

Computerized image encryption is a standout amongst the most vital systems for image data. The image encryption methods chiefly incorporate compression approach, cryptography system, chaos strategies, and DNA procedures etc. Cryptography and chaos have some regular peculiarities, which is debated in consequent segment. With the progression of portable correspondence technologies, the usage of varying audiovisual data in account with textile data gets to be more common than the past. Cryptography methodologies are in this way essential for storage of secured media content and circulation over open systems, for example, the web. A conventional approach to oppose statically and differential cryptanalysis is to utilize transformation and dispersion on the other hand.

Chaotic cryptography depicts the utilization of chaos hypothesis (specifically physical dynamical systems working in chaotic administration as a component of correspondence methods and processing algorithms) to accomplish diverse cryptographic assignments in a cryptographic system.

The ability of creating truly perplexing examples of conduct is an astonishing characteristic of chaotic systems. This is carried out from straightforward genuine systems or in recreations from low dimensional systems given by a little set of development mathematical equations. This quality has made them especially valuable for application in a wide variation of restraints, for

example, science, commercial concerns, engineering and others. Chaotic systems are utilized to create, reproduce, support or control diverse techniques enhancing their execution or giving a more suitable yield, in these sort of applications.

The utilization of chaos in cryptography appears to be very regular, as its characteristic properties unite it specifically with cryptographic qualities of perplexity and dispersion. This thought is available in Shannon's works (Shannon, 1949), much sooner than the expression "chaos" showed up in logical writing. Furthermore, chaotic dynamical systems have the focal point of giving qualitatively straightforward systems to produce deterministic pseudo arbitrariness. This could be the guarantee of creating more straightforward or better arbitrariness regarding execution for cryptography.

At this point, the historical backdrop of chaos based cryptography is more than twenty years long. To start with, a few works show up in the 80's, however it is in the 90's, when chaotic cryptography truly profits off. As an outcome, chaotic cryptography has been a dynamic exploration field yet with minimal effect in traditional cryptography.

IV. PROPOSED SYSTEM

Multimedia communications; such as, images audio, and video has become significantly more important, since communications of digital products over the network (wired/wireless) has expanded. There is therefore, an increasing need to secure data and its transmission and also to identify the required levels of security depending on the purpose of the communication. A wide variety of cryptographic algorithms have been proposed to meet these requirements. Traditional ciphers methods are less efficient in securing real-time multimedia data encryption systems and exhibit some drawbacks and weakness in high stream data encryption. The availability of a high computation machine may allow a brute force attack against these types of cipher. Furthermore, for cryptosystem applications that require high computation processes; large computational time and high computing power, as in the encryption of large-scale image encryption are seen to suffer from low efficiency levels. Therefore, these encryption algorithms are not appropriate for many high-speed applications because of their slow real-time processing speed and some other issues related to the processing of different data formats. Current research into the development of new chaotic or hyper-chaotic systems is highlighting the benefits of real-time encryption and communication applications. They show that chaotic systems are good schemes for designing cryptosystems, which have preferable characteristic. Within this research a hyper-chaotic system is proposed using a one-dimension logistic chaotic system and three-dimension Hénon chaotic system. The proposed hyper-chaotic system is applied on image encryption.

Chaotic Theory

All systems can be basically divided into three types:

1. Deterministic systems:
These are systems for which for a given set of conditions the result can be predicted and the output does not vary much with change in initial conditions. Examples are computers.

2. Stochastic/random systems:
These systems,which are not as reliable as deterministic systems. Their output can be predicted only for a certain range of values. Examples are genetic algorithms.

3. Chaotic systems:
These systems are the most unpredictable of the three systems. Moreover they are very sensitive to initial conditions and a small change in initial conditions can bring about a great change in its output. Examples of chaotic systems are the solar system, population growth, stock market, and the weather. Chaos is derived from the Greek word “XĮos”, which is meaning a state without predictability or order. A chaotic system is a non-linear, dynamical, and deterministic system which has high sensitive to initial conditions of the system. Chaos system is deterministic system with small change in input results in enormous change in the output, so the system looks as if it is random and prediction becomes impossible (it looks like a noise). It is like butter-fly effect. Due to these properties, chaos theory has been used in cryptography/encryption. In this work, chaotic theory is used for providing security at HW level.

DNA encoding and decoding for images

A DNA sequence contains four nucleic acid bases A(adenine), C(cytosine), G(guanine), T(thymine), where A and T are complementary, G and C are complementary. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary. By using four bases A, C, G and T to encode 00, 01, 10 and 11, there are 24 kinds of coding schemes. But there are only 8 kinds of coding schemes satisfy the Watson–Crick complement rule (Watson and Crick, 1953), which are shown in Table 1.In this paper, we use the DNA code to encode the color image. A color image can be divided into three channels: Red channel, Green channel and Blue channel. For the 8-bit single channel image, each pixel can be expressed as a DNA sequence whose length is 4 (its binary sequence’s length is 8). For example, if the first pixel value of the Red channel image is 173, convert it into a binary sequence is [10101101]. By using above DNA encoding Rule 1 to encode it, we can get the DNA sequence [CCTG]. Whereas, using DNA encoding Rule 1 to decode the above DNA sequence, we can get a binary sequence [10101101], but if we use DNA encoding Rule 2 to decode the same DNA sequence, we get another binary sequence [01011110]. Obviously, it is also a simple way of encryption.

Hénon map

The Hénon map is one of the discrete dynamical systems that exhibit chaotic behaviors. The Hénon map is defined by two equations and depends on two parameters *a and b*, and the system exhibits a strange attractor for $a = 1.4$ and $b = 0.3$ (system equation (3)). A Hénon map takes one point (x, y) and maps this point to a new point in the plane.

$X\ n+1 = 1- a\ (Xn)\ 2+Y\ n$

$Y\ n+1 = b\ Xn$ (3)

The Hénon map is very sensitive to initial values, and different chaotic sequences with large translation can be generated by the adjustment of parameters and initial values indicating that is suitable for generation of cryptographic functions, due to the capability of generating massive chaotic sequences; and the is a periodic and non-convergent, so it has excellent pseudo randomness and unpredictability.

Three-dimensional Honen map as it refers to system equation (4).

$x\ n+1 = a - yn2 – b\ z\ n$

$y\ n+1 = x\ n$ (4)

$z\ n+1 = y\ n$

The Hénon map generated from this chaotic attractor is more complex than the maps from other chaotic attractors; when $1.54<|a|<2$, $0<|b|<1$.

Generation of the secret key

In Chen's hyper-chaotic system, the initial values x1, y1, z1 and q1 can be seen as the secret keys. After encoding the image with DNA encoding rules, we can get three Hamming distances for color image's channels. In this paper, we transform three Hamming distances (H) into three decimal numbers, add them to three initial values of Chen's hyper-chaotic system one by one, and finally, get \ three new initial values of Chen's hyper-chaotic system. Pseudocode of generating one new initial value x1 of Chen' system is shown as follows:

if H > 1 **then**

H←H/10

else

x1←x1 + H

end if

V. RESULTS

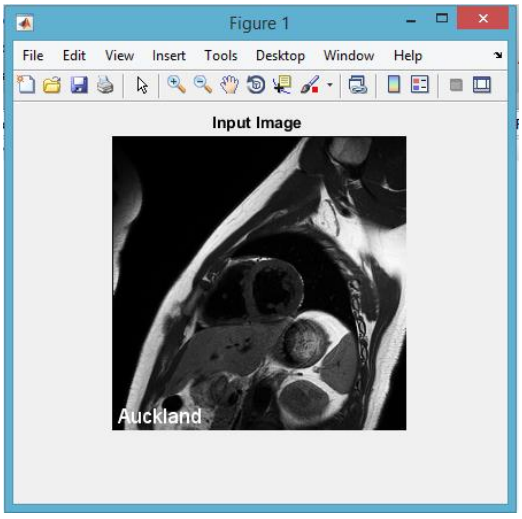

Fig.1: Input Image

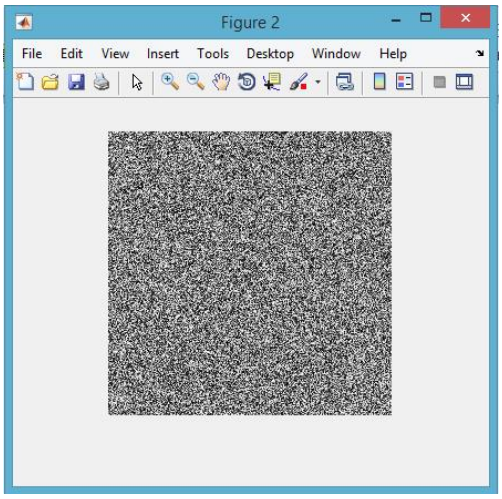

Fig.2: Encrypted Image

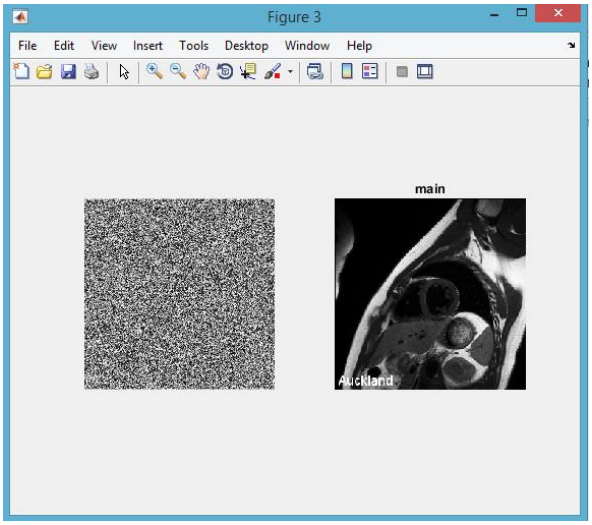

Fig.3: a) Encrypted Image b) Decrypted image

VI. CONCLUSION

In this paper, we proposed a novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. In this algorithm, the positions of pixels are scrambled by Chen's hyper-chaotic system and the pixel grey values of the original image are scrambled by DNA sequence addition operation. We proposed a new method to improve the ability of resisting differential attack by using Hamming distance to generate the secret keys. Through the experimental results and security analysis, we find that our algorithm has good encryption effect, larger secret key space and high sensitive to the secret key. Furthermore, the proposed algorithm also can resist exhaustive attack and statistical attack. All these features show that our algorithm is very 17 suitable for color image encryption.

VII. REFERENCES

[1]. Huang, Q. and Liu,J., "Secure Image Encryption Technique Based on Multiple Fresnel Diffraction Transforms", in International Conference on Wireless, Mobile and Multimedia Networks, 2006, pp. 1-4.

[2]. Xin,Y. Tao, R., and Wang,Y., "Image Encryption Based on a Novel Reality-Preserving Fractional Fourier Transform", in first International Conference on Innovative Computing, Information and Control, 2006, vol.-3, pp. 22-25.

[3]. Hwang,H., Han, P., "A Novel Wavelet Transform Algorithm for Image Encryption", in Australian Conference on Optical Fiber Technology & Australian Optical Society, 2006, pp. 1.

[4]. Zhang,C., Wang, J., Wang, X.,"Digital Image Watermarking Algorithm with Double Encryption by Arnold Transform and Logistic", in Fourth International Conference on Networked Computing and Advanced Information Management, 2008, pp. 329-334.

[5]. Wei,Z.,Zhi-gang,C.,Yue-li, C., "Image Data Encryption and Hiding Based on Wavelet Packet Transform and Bit Planes decomposition", in 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM '08, pp. 1-4.

[6]. Yoshimura,H. and IWAI,R., "New encryption method of 2D image by use of the fractional Fourier transform", in 9th International Conference on Signal Processing, ICSP 2008 , pp. 2182-2184.

[7]. Zhao,H., Ran,Q.,Ge, G., Ma, J., Tan, L., "Image Encryption Based on Random Fractional Discrete Cosine and Sine Transforms", in First International Workshop on Education Technology and Computer Science, ETCS '09 ,vol. 1, pp. 804-808.

[8]. Chuang,C.,Lin,G. "Adaptive Steganography-based Optical Color Image Cryptosystems", in IEEE International Symposium on Circuits and Systems, ISCAS 2009, pp.1669-1672.

[9]. Zhou,N., Dong, T. , "Optical image encryption scheme based on multiple parameter random fractional Fourier transform", in Second International Symposium on Electronic Commerce and Security, ISECS'09, vol. 2, pp. 48-51.

[10]. Zhang,L., Wu J.andZhou,N., "Image Encryption with Discrete Fractional Cosine Transform and Chaos", in Fifth International Conference on Information Assurance and Security, IAS '09, vol. 2, pp. 61-64.

[11]. LANG,J., TAO,R. and WANG,Y., "The Generalized Weighted Fractional Fourier Transform and Its Application to Image Encryption", in 2nd International Congress on Image and Signal Processing, 2009, pp. 1-5.