Computer

Technology, Computer

Considering digital image features with high volumes and video data, especially in real-time applications, the use of classic encryption methods like DES, AES, is not efficient in terms of being time consuming. In this article, a new method is proposed to encrypt digital images, using chose systems and utilizing DNA patterns. A central Idea In the method suggested is to produce a pseudoscience DNA strand using chaos functions, which an encrypted strand Is created, using the random strand and the strand produced from the main Image. Also, In the method, multiple tables are used;

In the article how to create and use these tables are addressed. One of benefits of the method Is the small volumes of data that are accessed by utilizing DNA patterns. Experimental results and security assessment experiments Indicate that the method suggested has an Ideal level of security. With development of computer networks and the Increasing use of Internet, the discussion of security In transferring data has been put forward as one of Important subjects. The reason for It Is the accessibility of data in Internet, and their easy access by authorized and unauthorized people.

Data jackets in Internet pass several intermediate public networks before they reach the target; this makes it easy that other people access data. In case of lack of protection of these data packets, it is impossible to work with Internet. One of methods of data protection is to encrypt them. By data encryption, if there is unauthorized access to data by people, the possibility of using data will be impossible. Also, with development of new applications, especially in commercial, military areas; video conferences , , the need for quick and secure systems for digital images is increasing more and more.

Recently, many algorithms [J have been presented, which have been suggested as methods of digital image encryption. In general, encryption algorithms and techniques are classified in groups including compression methodology, modern cryptography mechanism, chaos techniques, DNA techniques, etc. Different techniques and methods have been proposed to encrypt data. Techniques based on mathematical concepts are among them 0. These techniques are generally based on Arnold transforms, space curve concepts, or other mathematical concepts.

Also there are methods based on secret sharing concepts 0 suggested by Shaman in 1979. Of ours, these methods have rarely been used In practice. Encryption methods based on compression 0 are other methods proposed for digital Images, which are usually based on compression like scan language 0, or techniques based on vector quantization 0. Also, there are techniques presented as modern techniques Including DES (Data Encryption Standard) 0, AES (Advanced Encryption Algorithm) 0, IDES (International Data Encryption Standard), or RASA [I.

Of course, these methods are not appropriate for real-time Image encryption In terms of time and speed. Transform domain-based Image encryption technique Is a method and technique hat Its central Idea Is based on an operation performed In transform domain. This operation is based on techniques like chaos [I, Fourier transform [I, and or wavelet transform O, etc. Today, one of methods used more is techniques based on nonlinear and ensured systems like chaos systems [I. Test systems, in terms of strong sensitivity to the stating point, are efficiently used to encrypt images.

Also, using predict and analyses; this has helped with the increasing use of the method in encryption. In general, it can be claimed that the use of chaotic systems can improve encryption system security. Recently, DNA patterns-based methods have attracted the attention of investigators in the encryption area 0. Of course, biologic methods based on this technique are not currently developed; however, methods based on DNA computing have been proposed 0 that use DNA patterns in the encryption area. In this article, a new method is proposed to encrypt digital images, based on chaos systems and utilizing DNA patterns.

In the method, values related to pixels are converted to a DNA strand, and by combining another strand created randomly, the encrypted strand of the image is obtained. Multiple tables are used to convert the plain strand to the cipher strand that how to design and use them will be examined. Analyses and tests conducted on the strand and encrypted image indicate that the suggested method is resistant to cryptanalyst attacks and has higher security. In section 2, basic concepts and a summary of encryption based on chaos systems are explained.

Concepts of use of DNA patterns are addressed in section 3. In section 4, the suggested method is discussed and explained. In section 5, a model related to the method will be presented. Security analyses will be examined in section 6. Chaos systems are nonlinear systems that have more sensitivity to initial conditions and show pseudo-random behavior. Chaos signals are similar to noise in appearance, and in spite of displaying random behavior, being absolutely definitive- having initial values and mapping functions, the same perilously produced values can be produced.

They will be in the chaos state if these systems satisfy the Lawfully exponential equation conditions. The pseudo-random feature in these systems has made them outstanding for encryption. In 1993 Hays and coworkers suggested chaos systems for data tanager 0. However, many encryption algorithms and methods based on chaos theory have been designed and suggested 0. Most of encryption systems use chaos functions to produce a sequence of random numbers. Combining in special algorithms, these pseudo- random numbers convert plain data to cipher data.

Image encryption is different from encryption of other data that many correlations among pixels can be pointed among others. Therefore, the use of more efficient methods than classic methods should be considered. In recent years, many methods based on chaos functions have been proposed to encrypt images C]. Although a lot of research has been conducted in the chaos system encryption area and many methods have been proposed, many methods have been designed to attack these systems and decode data, due to weakness in their design 0.

Therefore, these systems and the design of efficient methods for them have currently become a main subject in the encryption area. One of main stages in chaos-based encryption systems is to choose a mapping function. The correct and appropriate choice of the mapping function, and examining and analyzing initial conditions and areas in which he function has chaotic features cause increased efficiency of encryption system and more stability of encrypted data against hackers.

In the system suggested in the article, the logistic mapping function, which is one of simplest and of effective features, was chosen. This function is one of functions of nonlinear systems suggested by Pierre François Overhauls as a model in 1838. In 1947, Lam and Von encryption, instead of s-box tables, the logistic function was used. The logistic function is defined as Relationship 1 where a is the function parameter and shows efferent behaviors based on different values of the parameter.

In the article, values of the parameter were chosen in an interval (309996, 4) so that its chaos features can be used. Also, for beginning we need an initial value ox. The initial value that must be in an interval (0, 1) can be calculated by a key value in encryption system. How to calculate the value in the suggested system will be explained. Knowing the initial values of a, and starting with the point, a sequence of numbers between O and 1 is produced. These pseudo-random numbers can be used in encryption algorithm.