ABSTRACT

Multimedia formats such as text, images, audio and video are currently being stored and distributed on a wide range of networks and devices. When an unauthorized user gains access to the system, it is quite easy to copy and redistribute such information. Cryptography has therefore become a necessity to protect the content against unauthorized access. The requirements of encryption techniques vary widely for different forms of data; the demands of image encryption methods are challenging than those of text encryption owing to the intrinsic characteristics of bulk data and elevated redundancy. Not only are the encryption techniques required to be secure and fast, the cipher also needs to be as easy to handle, store and transmit as the data.. Generally in image encryption algorithms, pixel values are substituted and/or scrambled to reduce the correlation among them when external keys are used.

Although It has been shown in studies that scrambling and substitution operations alone are not sufficient to achieve a secure cipher. The difference between ciphers must be significant even when a slight change is introduced in the key or input image. This is only possible if the avalanche effect in encryption algorithm is significant. Further, the key space of the algorithm should be large enough to prevent cracking it through brute force. A good encryption algorithm is one, which has both confusion and diffusion properties for improved security. Chaos is being widely used in image encryption techniques by researchers to meet the demands of a good encryption algorithm. Chaos being extremely sensitive to change in initial conditions, ergodicity and its mixing property makes it the popular choice for cryptography. Deoxyribonucleic Acid (DNA) cryptography is another emerging technique which is a potential alternative for efficient and fast image encryption. A number of DNA and chaos based image encryption techniques have been proposed and analysed. Both DNA and chaos based encryption approaches have been found to focus on speed and efficient storage, security is still not addresses satisfactorily. They are found to be week against attacks like known/chosen plain text attack, noise attack and sensitivity for change in key or plain text. Therefore, the challenge for researchers has been to design an efficient image encryption technique which can also resist various security threats.

Once a user sends the data through communication channels, it is not possible for the user to know whether the data has reached the destination successfully and securely. It is also important to focus on secure text data communication as it is the most common and basic form of communication. The Double Reflecting Data Perbutation (DRDP) method and hashing are used in the suggested system to provide text data security. Using a key K, the encryption of Plain text (P) gives the Cipher text (C) & decryption of C results in P. It consists of data encryption and decryption using Shared-Secret Key (SSK), Session Key (SK), and Intermediate Key (IK). A variable number of the SK and the IK is created based on the length

of the P. Using DRDP method and hashing function with the length of the P, the variable number of a SK and an IK is generated. The proposed system uses message digest providing integrity with the added advantage of authentication, as only the sender and receiver know the SSK.Thus message digest not only handles integrity but also achieves authentication.

Eventhough the cryptographic algorithms are suitable for text encryption it may not be appropriate for other multimedia data such as image data due to their high redundancy and large volume. Highly personal and sensitive image data is handled in fields such as medical & military, it is therefore vital to secure these image data before transmission or distribution. Image encryption is a must in such cases to improve the security. This has led to the need for new and better techniques of image encryption.

The investigation focuses on improving the security with a blend of the chaotic model and cryptography. Chaos is the study of nonlinear and deterministic systems that are highly sensitive to the initial conditions and parameter values. A novel key generation algorithm using Enhanced Logistic Map (ELM) is proposed, which will be more secure. The complete procedure involving encryption and decryption with ELM can be called as Enhanced Logistic Tent Map (ELTM) algorithm. The suggested encryption algorithm can withstand to certain attacks also the correlation between the pixels are broken.

In image encryption, the effectiveness of cipher largely depends on the quality of the 'key'. If the quality of the key is low it is not possible to provide the required level of security even with sophisticated encryption and decryption algorithm. The image transmitted through the communication channels are secured with the new key generation algorithm that uses an optimization technique. If the size of the block is n×n, there are n2 pixels and (n2)! possible arrangement of pixels in a block. The study uses a suitably modified Particle Swarm Optimization (PSO) algorithm to generate a secure and suitable key for the image. During encryption, it is also critical to choose the best pixel that will reduce the correlation between the neighbouring pixels. Thus statistical analysis have been done and it produce good results and also it can withstand to certain attacks.

Mobile devices are becoming a computing platform to perform financial transactions that requires secure authentication. Biometric authentication has been proven to be safe for financial transactions. The content based biometric image data is considered for data authentication in this investigation. The secure cryptographic model captures the user's image during the transaction and uses it for key generation and exchange. The problem of personal identification depends on the various factors such as illumination, skin tone, complex background and other such factors. The features like face location and facial component positions can also be used for the user identification.

The system scans the face from the device and the facial components are fixed for further detection. The components detected are subjected to normalization or recognition directly. Multi-level authentication is performed through verification of face and IRIS data from

Quality-Face/IRIS Research Ensemble (Q – Fire) dataset as it has better accuracy. After the successful authentication, the transaction server generates an OTP. The Elliptical Curve Cryptography (ECC) is used for the process of encryption and decryption and the user features obtained from self-image is used as key. The performance of the system is evaluated in both identification and verification scenarios and it proves better.

Biometric technologies are playing a vibrant role in various security applications. An automatic recognition system can identify a person by determining their specific characteristics. In recent times biometric systems are being used as one of the primary methods for secure authentication. The unimodal biometric systems are susceptible to variety of attacks; therefore the requirement for a better system is increasing.

To reduce the error rate, the multimodal biometric systems can be employed which integrates two or more biometrics traits. The fundamental challenge in designing a biometric template protection scheme is to overcome the large intruder variability among multiple acquisitions of the same biometric trait. The performance of a multi-biometric cryptosystem is assessed by its accuracy.