Abstract

Cryptography is the practice and study of techniques to hide information in storage or transit for secure communication in the presence of adversaries. Private key cryptography uses the same cryptographic keys for both encryptions of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. Authentication is a process that ensures a user's identity. Steganography is the process of hiding information using a cover carrier like text, image, audio, and video. In the last two decades, researchers have derived new algorithms and information hiding models using cryptography, authentication, and steganography. There is a scope to develop a security toolkit by combining newly implemented independent models using cryptography, authentication, and steganography all together in a cascading manner which provides better security for transmitting data as compared to the standard algorithms.

The basic objective of the work is to design an integrated ciphering system or a so called, 'security toolkit'. Such a system has been formed by combining a set of newly developed independent bit-level ciphering protocols. Each of these protocols ultimately has acted as the 'building block' for that implemented 'security toolkit'. For the purpose of assessing each 'building block' which has been developed during the work, different standard algorithms and parameters have been used.

The contribution of the abstract of this research is threefold. In the first part, 'user authentication building blocks' have been introduced based on CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) code generated from personal information and OTP (One Time Password) formulated on biometric image.

Three authentication schemes have been implemented namely “CAPTCHA Code based on User Personal information and Likings (CCUPL)”, “Secret Value based on Randomized One Time Password (SVROTP)” and “Numeric and biometric Image-based One Time Password (NIOTP)” for ‘authentication building blocks’.

CAPTCHA or OTP generation time, their randomness and how they provide security over different network attacks have been considered as standard parameters for assessing the performances of newly implemented schemes.

The distribution of the private key without interpretation is very hard to achieve. So, in the second part, an attempt has been made to design a predefined secret procedure to retrieve the secret value from the private key, as well as securing both the actual private key value and the secret procedure from unauthorized access at the time of encrypting character based plain text. Both the encryption and decryption have been done by the secret value derived from the private key. Seven text encryption algorithms have been implemented namely “Prime number with Alphabetic Group based text encryption (PAG)”, “Palindrome number with Alphabetic Group and Operator based text encryption (PAGO)”, “Multiple Operator and Even Odd position based text encryption (MOEO)”, “Multiple Operator and ASCII Value based text encryption (MOAV)”, “Multiple Operator and number of Zeros and Ones based text encryption (MOZO)”, “Armstrong and Perfect number with Cipher Sequencing based text encryption (APCS)” and “Amicable number with Cipher Sequencing based text encryption (ACS)” for ‘text encryption building blocks’.

Multiple parameters like time requirement for phase wise (encryption + decryption) execution, degree of freedom value, formulation of the structure of private key being used, Pearsonian chi-square value have been considered for measuring the performance of ‘text encryption building blocks’. The result of each of the algorithms has been compared with standard AES (Advanced Encryption Standard), Triple DES (Data

Encryption Standard), Twofish, Blowfish and Serpent algorithms where satisfactory outcomes have been observed.

In the third part, image partitioning, key based encryption, digital enveloping and user defined steganographic scheme based new ‘image encryption building blocks’ have been introduced. Three new image encryption schemes have been implemented namely “Even Odd block based Digital Enveloping scheme (EODE)”, “Cumulative Image encryption using Digital enveloping, Key based encryption with image Partitioning (CIDKP)” and “Cumulative Image encryption using Steganographic scheme with Pixel repositioning (CISP)” for ‘image encryption building blocks’.

Encryption speed, cryptographic security, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Universal Image Quality Index, Bit Error Rate (BER), Correlation Coefficient (CC) and Normalized Cross Correlation (NCC) have been considered as parameters for measuring the performances of the implemented ‘ image encryptions building blocks’.

Based on all these and few more new parameters, the performance of each ‘building block’ has been compared with two selected standard existing protocols. After the successful completion of designing and developing all the ‘building blocks’ in an independent manner, all such blocks have been cascaded by formulating proper schematic characteristics as well as operational characteristics. A satisfactory outcome of implementing this ‘security toolkit’ in a stand-alone system has been experienced, which has indicated that the successful completion of this chain of actions has been ultimately reached to the end of this research work.