Chapter 2

Early Work related to Current Research in User Authentication and Data Encryption

2.1. Overview

Many innovative and new encryption and steganographic approaches from the domains of user authentication, text encryption and image encryption have been developed in the last few years. In the current chapter, advancement of encryption and steganographic methods from text, image and user authentication domain are reviewed. The focus is imposed on the specific region of the mentioned domains relating to the interest of the current research work.

Section 2.2 reviews data encryption approaches. Section 2.3 and 2.4 reviews CAPTCHA and OTP based authentication schemes. Text encryption techniques are reviewed in section 2.5. Section 2.6 goes through different approaches of image encryption. Steganographic techniques are reviewed in section 2.7. Conclusion has drawn in section 2.8.

2.2. Data Encryption

DES (Data Encryption Standard) [7][52] was considered as the first encryption standard. DES was implemented based on the algorithm Lucifer which was introduced by IBM. DES was considered as standard in the year 1974 by NIST (National Institute of Standards and Technology). DES is a block cipher which became insecure as different attacks and techniques have breached DES from its time of origin.

Advanced Encryption Standard (AES) [29][57] is a symmetric block cipher which was considered as a replacement of DES. AES is also known by its original name Rijndael. AES was selected by NIST in the year of 1997 as the best encryption standard from a contest. AES supports larger key size and it is faster than DES. The only known effective attack against AES is Brute Force attack where the combinations of characters are tested to breach the encryption.

Triple DES or 3DES [82] is a block cipher where the symmetric secret key is present. Triple DES is an advancement of DES. In Triple DES similar encryption techniques are followed as of basic DES but it is executed for three times. Thus the encryption level is higher. Triple DES was published in 1998. Security level provided by Triple DES is higher compared with regular DES though the encryption speed is less.

Serpent [30] is a block cipher which supports symmetric key. High security is ensured by serpent where it lacks speed. Serpent algorithm was designed by Anderson, Knudsen and Biham. Large key size and 128-bits block size are supported by the serpent. High security provided by serpent though its speed is low. Still, serpent manages to run faster than DES.

Blowfish [98] is a block cipher which supports symmetric key. Blowfish was considered as a fast alternative technique over other algorithms in 1993 by Schneier. As Blowfish is available in public domain so it is freely accessible. Good encryption ratio is produced by blowfish algorithm and full Blowfish provides ultimate security over unauthorized access. As the structure is simple and rounds are less so Blowfish is a fast cipher.

Twofish [57] is a block cipher with a symmetric key. Twofish was developed as a combination of flexibility and speed in 1998. Twofish was originated from different algorithms like SAFER, Blowfish and Square by Schneier. Free access to Twofish is possible as it is available in the public domain. Twofish is a very fast technique and it has a good combination of conservative structure and flexibility.

International Data Encryption Algorithm (IDEA) [13] was introduced by Lai and Massey of ETH Zurich. It is a block cipher and described in 1991 for the first time. IDEA provides high security level where 64-bit blocks of plaintext and ciphertext and 128-bits key are supported. The fundamental of IDEA is based on the applying of operations from different algebraic groups.

RC5 [52] is a block cipher algorithm based on a symmetric key which was developed by Rivest in 1994. RC5 has a very simple algorithm which supports variable key size (0-2040 bits), the number of rounds (1-255) and block size (32, 64 or 128 bits). Data dependent notation is applied in RC5. XORs and modular additions are also applied for RC5 as a component.

RSA [56][57][97] is widely used public key cryptosystem which was introduced by Rivest, Shamir, and Adleman in 1977. A single round of encryption is applied for RSA where it supports variable length key size (1024 - 4096 bits). RSA is certified from different standards like PKCS#1, ANSI X9.31 and IEEE 1363. In RSA a public encryption key and a secret decryption key is applied where the decryption key is different from the encryption key.

2.3. CAPTCHA based User Authentication

In the year 1999, Biddle et al. [81] introduce the concept of image based CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) originated from the idea of graphical password where the concept of using a predefined image as password generates the idea to consider images for CAPTCHA authentication. The security of this implemented knowledge driven authentication procedure is higher than the existing authentication approaches based on the text.

Chew et al. [51] describe the idea of Image CAPTCHA for the first time. Multiple images or multiple photographs are used for generating the image CAPTCHA. The main focus is to construct image CAPTCHA based on image recognition where the

previously selected images have to be recognized by the user. An Image database is used to implement Image recognition CAPTCHAs.

Elson et al. [33] discuss about image CAPTCHA system where a closed image database is used as a source of images. An image pool consists of closed images is available and a user has to choose the proper image. The main drawback of this system is that as the numbers of available options for the solutions are so less that single random guessing may achieve success with very high probability.

Raj et al. [3] introduce the idea of imposing sequences on image CAPTCHA. Two levels of securities are present in this approach. In the first level, proper images have to be recognized by a user and in the second level, logical sequences for all the recognized images are to be defined by the user. The security of this scheme is higher though the volume of computation is high.

Yalamanchili et al. [105] represent a text based CAPTCHA where the CAPTCHA is generated based on the Devanagari script. This approach is not so user friendly and the knowledge based approach for authentication is not considered here.

Chowdhury et al. [64] introduce a knowledge based CAPTCHA scheme which supports user friendly environment and diversity on question selection which has to be answered. A user study is available for the performance assessment of the implemented system. User knowledge regarding the answers of provided questions is the restriction for the implemented scheme.

Nguyen et al. [113] represent a text based CAPTCHA scheme where the user has to identify and recognize the character with its location in all the characters present in the CAPTCHA. The drawback of the scheme is that, as the character recognition may be possible for an automated program so fetching the location of a specific character is not very hard to achieve.

Subramanyam et al. [67] describe an idea of image based CAPTCHA where the user has to recognize and select appropriate one image from four images based on questions associated with it. Security level for the implemented scheme is not as high as the selection of only one image for a single question is the only authentication criteria.

Angre et al. [1] represent the concept of image based CAPTCHA where the user has to identify single or multiple images depending upon the questions provided by the CAPTCHA scheme. Security of the implemented scheme is not so high as the implemented scheme is depends on image recognition.

Singh et al. [71] describe a random number based CAPTCHA scheme where the authentication is based on the insertion of the random number generated from the CAPTCHA authentication scheme. Security of image based CAPTCHA approaches is not present here.

Mankhair et al. [101] represent visual cryptography based image CAPTCHA authentication scheme where the original image CAPTCHA is decomposed into two shares and they are kept in the separate database server (one for keeping user share and other for keeping server share). CAPTCHA is generated only when both the shares are simultaneously available. The main drawback of this system is that the user has to wait for several periods of time to get the reconstructed CAPTCHA and the implementation cost is higher as multiple database servers are needed.

Padhye et al. represent [108] a new idea where text password and graphical password based CAPTCHA scheme is implemented together. A user has to select multiple images which are previously inserted at registration time form the available images for authentication. As graphical password based style is followed here so the authentication is depended only on the predefined images which are the restriction of the implemented scheme.

Goswami et al. [24] describe new image CAPTCHA scheme which is implemented on facial expressions, features and recognition of faces. Two faces which are matched based on facial expressions and features that have to be identified for validating user login. It is hard to identify two faces from all available faces which are carrying similar types of facial expressions.

Tang et al. [60] represent an image based CAPTCHA approach named Style Area CAPTCHA where the idea is based on multiple concepts of pixel level segmentation, understanding of semantic information and technique of deep learning. The complexity and the processing are higher for implementing this scheme.

Anil et al. [37] discuss an image based CAPTCHA which provides randomly chosen images with the facility of controlling the distortion of images. The scheme accomplishes the security level from unauthorized access is not as higher as compared to the existing standard CAPTCHA schemes.

Table 2.1 represents the comparison between different CAPTCHA based authentication schemes.

Table 2.1: Comparison between Different CAPTCHA based Authentication Schemes

Authors	**Year of Publications**	**Core Idea**	**Advantages & Limitations**
Biddle et al. [81]	1999	Image CAPTCHA based on a graphical password.	Considerable level of security but the unavailability of an image database
Chew et al. [51]	2007	Image CAPTCHA based on closed image database	Considerable level of security but less available options

Raj et al. [3]	2010	Sequences based image CAPTCHA	High security but high volume of computation is needed
Yalamanchili et al. [105]	2011	Text CAPTCHA based on Devanagari script	Moderate level of security but not user friendly
Chowdhury et al. [64]	2013	Knowledge based CAPTCHA	High security but limitations of user knowledge
Nguyen et al. [113]	2014	Text CAPTCHA based on character recognition and location of character	Simple but provides less security
Subramanyam et al. [67]	2015	Image CAPTCHA based on recognition and appropriate image selection	Moderate security but less option for image selection
Angre et al. [1]	2015	Image CAPTCHA based on image identification as per questions	Simple but provides less security
Singh et al.[71]	2015	Random number based text CAPTCHA	Very Simple but security is less
Mankhair et al.[101]	2016	Visual cryptography based image CAPTCHA	High security but high response time and implementation cost
Padhye et al. [108]	2017	Text password and graphical password based CAPTCHA	Moderate level of security but dependency exists on the predefined image

Goswami et al. [24]	2017	Image CAPTCHA based on facial expressions and recognition of faces.	High security but hard for a user to identify close similar image based on features.
Tang et al. [60]	2018	Image CAPTCHA based on pixel level segmentation and deep learning technique	High security but Highly complex with higher implementation cost
Anil et al. [37]	2018	Image CAPTCHA based on random image	Moderate level of security but high implementation cost

2.4. OTP based User Authentication

Lee et al. [118] discuss a technique about generating OTP (One Time Password) based on Ping Pong-128 bit stream cipher protocol and random digit selection. The scheme provides standard security for OTP generation and it has a lightweight algorithm as it based on Ping Pong cipher. The limitation of this scheme is that sufficient level of security is not present at the time of distribution of OTP.

Hsieh et al. [115] represent an OTP based authentication scheme where the volatile OTP is generated based on the information of the location of mobile phone and time of accessing the internet by that mobile phone. Restriction of the scheme is that accessing of phone location is hard if the network connection becomes poor.

Parmar et al. [31] represent an idea of user authentication based on the combined techniques of Image and OTP based authentication. Image based authentication is carried out by recognizing the previously chosen image from a grid of images and HMAC based OTP implementation is included in this scheme. As a combined approach the security level is increased but the scheme has all the limitations which are present in an HMAC based OTP scheme.

Kumar [46] discusses an OTP based authentication scheme where OTP is constructed with a combination of image and numeric content. As the distribution of OTP is carried out through the public network without any encryption so the scheme is not so secured.

Hussein et al. [42] represented a user authentication scheme based on OTP based authentication where the identification of both the user and the mobile device are validated before distribution of OTP. User identification is validated based on personal information and the mobile device is identified by International Mobile Equipment Identity (IMEI). The main drawback of this scheme is that personal information of the user has to be shared through a public network to the server for validating his/her identity.

Huang et al. [119] represent an OTP scheme where a unique passcode is generated for authentication for each attempt. The sequence number and the time stamp value define the passcode value. Various attacks like keyboard monitor, memory scan, software clone are not been protected by this scheme.

Hamdare et al. [89] describe a combined OTP based authentication scheme where a secure key is combined with the OTP and the entire value is transformed to transaction password by the help of RSA algorithm. Distribution of the OTP is not needed as a similar activity is done both in server end and in user end. The complexity of the scheme is higher as the same computation is carried out in both ends.

Saini [106] represents an OTP based authentication scheme where the idea of a genetic algorithm and elliptic curve cryptography are used. The implemented scheme is not so much secured compare to other OTP schemes.

Alsaiari et al. [26] introduce a combined graphical authentication scheme termed as "GOTPass" where the authentication is carried out based on one time password which

has to be inserted or typed depending upon the secret image's sequence and by following previously chosen format of the input. Multiple authentication schemes (OTP, graphical password) and multiple authentication modes (recall and recognition based) are applied in this current scheme which increases the security. A user has to keep more information regarding authentication in mind as compared to other existing schemes as multiple levels and mode of authentication is present in this current scheme.

Chow et al [116] discuss visual OTP based authentication scheme where a challenge response based style is followed. In this scheme, the challenge image is received on the mobile device's camera and the display of the mobile device is used for making the response of the user. The main limitation of this scheme is that the scheme suffers from man-in-the-middle attack and this scheme is not applicable to visually disabled people as well as for the mobile devices without a camera.

Vishwakarma et al. [70] introduce an authentication scheme where text based OTP is generated with the presence of a random image by using the SHA-512 algorithm. The entire result is encrypted by using Elliptic Curve Cryptography (ECC) and thus generates the final OTP. Cost of the scheme is higher compared to the security level provided by the scheme.

Sheshasaayee et al. [5] represent an OTP based authentication scheme where ciphertext is generated from OTP by lightweight cryptography algorithm and ciphertext is also hidden from unauthorized access by applying text steganography. Delivery of stego text is carried out as SMS to the authorized user. Personal Identification Number (PIN) is applied for OTP decryption at user end where a PIN is provided by the bank at the time of registration. The system is not so secured if the PIN is compromised which is the main drawback of this scheme.

Kaur et al. [69] describe an OTP scheme where online OTP is generated based on seed exchange where the seed is software generated token shared through the tunnel

of Transport Layer Security (TLS). Authentication is carried out based on the verification of OTPs in both server and user end where user end's OTP is generated from the shared seed value. As the user side OTP generation algorithm is easily available so if the seed value is compromised then the system might be breached.

Srinivas et al. [41] represent an OTP based authentication techniques where OTP is created from the random numbers which are generated based on the extracted features of an inputted image by the user. Selection of single feature of an image for OTP generation and considered image size has restricted the range of generated random numbers which are considered as OTP.

Mahto et al. [21] introduce a hybrid user authentication scheme based on One Time Password. The generation of the OTP is carried out using Elliptic Curve Cryptography and Iris Biometric. The security level provided by this scheme is higher as Elliptic Curve Cryptography provides better security using small key size and accurate user authentication is carried out by the reliable Iris Biometric technique. Sufficient amount of security is not present for the distribution of OTP for this present scheme.

Joshitta R et al. [96] represent new OTP based user authentication for accessing the data from cloud servers. Generation of OTP is carried out by applying Lagrange polynomial functions followed by the operation of Hash Message Authentication Code (HMAC). The Security level of this scheme is not as much higher as compared with existing OTP schemes.

Reyes et al. [9] discuss a scheme for providing secure OTP based on the Blowfish algorithm. A modified Blowfish algorithm is introduced which supports an input block of 128-bits with randomly defined execution rounds. As the performance of this scheme is higher over existing Blowfish algorithm so generated OTP is secured but no new technique is implemented for OTP generation in this present scheme.

Table 2.2 represents the comparison between different OTP based authentication schemes.

Table 2.2: Comparison between Different OTP based Authentication Schemes

Authors	Year of Publications	Core Idea	Advantages & Limitations
Lee et al. [118]	2010	OTP based on Ping Pong-128 bit stream cipher	Simple but provides less security
Hsieh et al. [115]	2011	OTP based on information of location and time of accessing	Moderate security but depends on network connectivity
Parmar et al. [31]	2012	HMAC based OTP implementation with image recognition	High security but the limitation of HMAC is present
Kumar [46]	2012	OTP based on image and numeric value	Simple but security is less
Hussein et al. [42]	2013	OTP based on the identification of user and mobile device	High security but private information has to be shared through the public network
Huang et al. [119]	2013	OTP based on sequence number and time stamp value	Simple but breached by different web attacks
Hamdare et al. [89]	2014	Combined secure key with OTP	High security but complex and high volume of computation
Saini [106]	2014	OTP based on genetic algorithm and elliptic curve cryptography	Easy to use but less security

Alsaiari et al. [26]	2015	OTP with graphical authentication	High security but high volume of information is needed for authentication
Chow et al [116]	2015	Visual OTP	Moderate level of security but suffers from man-in-the-middle attack
Vishwakarma et al. [70]	2016	OTP based on text, random image and Elliptic Curve Cryptography	Moderate security but higher implementation cost
Sheshasaayee et al. [5]	2016	OTP based cipher text	Easy to use but provides less security
Kaur et al. [69]	2016	OTP based on seed exchange	Moderate level of security but high computation cost
Srinivas et al. [41]	2016	OTP based on extracted features of image	Moderate security but consideration of less numbers of features for OTP generation
Mahto et al. [21]	2017	OTP based on Elliptic Curve Cryptography and Iris Biometric	High security but high computation is needed
Joshitta R et al. [96]	2017	OTP based on Lagrange polynomial functions and Hash Message Authentication Code.	Easy to use but less security level
Reyes et al. [9]	2018	OTP combined with modified Blowfish algorithm	Higher security for OTP distribution but response time is higher

2.5. Text Encryption

Mandal et al. [34] discuss a text encryption scheme depends on Fibonacci based Position substitution (FBPS) techniques in 2009. In this scheme Fibonacci number is used to substitute the positions of bits of plain text character and generate the cipher text. Security level is higher but the scheme needs larger amount of computation.

Mondal et al. [110] represent a block cipher algorithm based on symmetry key for text encryption. The encryption is carried out using the frame set where all the bits of the plain text's characters are placed in the frame set and then the bits are repositioned for generating the cipher text. The security of the scheme is not so satisfactory as compared with RSA or Triple DES algorithm.

Bhati et al. [104] discuss about text encryption scheme named Byte-Rotation Encryption Algorithm (BREA) which executes in parallel manner for reducing the encryption time. Parallel execution is carried out by rotating of bytes in different blocks of plain text with the concept of multithreading. The execution time is less for this scheme but the security level is not as much higher as compared with standard techniques.

Text encryption scheme based on ASCII value is represented by Singh et al. [109] in 2013. In this scheme cipher text is generated from the ASCII value of characters from plain text and value of randomize key which are combined together with the help of mathematical operations. As ASCII range is defined so only the key size and mathematical operation defines the security level for current scheme which is the limitation of this scheme.

Singh et al. [47] represent a text encryption scheme which is based on elliptic curve cryptography in 2015. In this scheme ASCII values of character from plain text are paired up and that value is taken as input for elliptic curve cryptography which

generates the cipher text. The scheme provides good level of security where the computation time is high.

A new text encryption scheme based on pseudo random number and non linier functions is discussed by Mishra et al. [61] in 2015. In this scheme the pseudo random number is taken as a secret key and non linier function is responsible for carrying out the encryption process. Security of this scheme is not as high as compared with existing standard algorithms as brute force attack may easily breach the scheme.

Galala [43] represents a text encryption scheme named Binary Count Encryption System (BCES) based on counting of bits from binary representation in 2015. In this scheme characters of the plain text is converted into ASCII value and that value is again converted into binary value. Number of similar bits, zeros and ones are counted and from there cipher text is generated. As the number of zeros and ones present in the binary representation of ASCII value of different characters are same for multiple numbers of characters, so the available range of cipher text characters are small which is main restriction of this scheme.

Pattanayak et al. [103] introduces new text encryption scheme based on extended Euclidean algorithm in 2016. In this scheme secret key is generated by extended Euclidean algorithm where secret key is applied on ASCII value of each characters of plain text for generating cipher text. Decryption is carried out by using inverse key which is generated by modular multiplicative inverse method. Security of this scheme is not as much higher as compared with standard encryption algorithms.

Kurniawan et al. [20] represent new text encryption scheme named Double Chaining Algorithm (DCA) based on the chaining process. This scheme supports symmetric key with a size of 128-256 bits. XOR operation is carried out for chaining process.
This scheme is less complex and it needs small time for execution but the achieved security level is not satisfactory as compared with existing schemes.

Mathur et al. [72] discuss text encryption scheme in 2016 based on AES where dynamic key selection is present. In this scheme the length of the key is 192 bits and 12 numbers of iterations are carried out to generate the cipher text. Thus the security level provided by the implemented techniques are satisfactory though the volume of computation is high.

Hybrid text encryption technique is represented by Sherkhane et al. [102] in 2017. The text encryption scheme is carried out based on armstrong number and color code. The decryption of the cipher text is done by using a secret key where key is generated by combining armstrong number and color code. The security level provided by this scheme is not as higher as compare with the existing OTP based authentication schemes.

Kumar et al. [44] discuss about new text encryption scheme based on DNA ASCII table in 2018. In this scheme first the mapping between numerical data and DNA sequences is established and it is converted into binary. Finally the binary data is transformed into DNA bases. The volume of computation is extremely higher for the present scheme.

Kottu et al. [94] represent enhanced text encryption algorithm based on DNA sequence, prime number and PI sequence in 2018. Two different keys are generated for encryption where first key is generated from PI sequence and second key is generated from DNA sequence. XOR operation is carried out between the binary value of characters of plain text and key value for encryption. Though the security provided by this scheme is in standard level but the scheme is very complex with high computation cost.

Muhammed et al. [65] discuss about an innovative text encryption method based on random number generation function in 2019. In this method generation of random numbers are depends on key and plain text. Random operations like random cyclic shifting, random mutation, dirty symbol random insertion and random permutation are

applied for ensuring the security of this scheme by converting plaintext's structure and relate to the key.Though the standard level of security is provided by this scheme but the complexity and computation cost is higher as compared with standard encryption schemes.

Table 2.3 represents the comparison between different text encryption schemes.

Table 2.3: Comparison between Different Text Encryption Schemes

Authors	Year of Publications	Core Idea	Advantages & Limitations
Mandal et al. [34]	2009	Text encryption depends on Fibonacci based Position substitution	Security level is higher but the scheme needs larger amount of computation.
Mondal et al. [110]	2010	Text encryption based on frame set of the plain text's characters	Simple and easy to implement but the security level is less
Bhati et al. [104]	2012	Text encryption based on rotating of bytes in blocks of plain text	Fast execution but security level is less
Singh et al. [109]	2013	Text encryption scheme based on ASCII value and randomize key	Considerable security level but security level is restricted by ASCII value range
Singh et al. [47]	2015	Text encryption scheme based on elliptic curve cryptography	High level of security but the computation time is high.
Mishra et al. [61]	2015	Text encryption scheme based on the pseudo-random number and nonlinear functions	Simple and fast but brute force attack may easily breach the scheme

Galala [43]	2015	Text encryption scheme based on the counting of bits from binary representation	Moderate security level but the available range of ciphertext characters are small
Pattanayak et al. [103]	2016	Text encryption scheme based on extended Euclidean algorithm	Fast but scheme provides less level of security
Kurniawan et al. [20]	2016	Text encryption scheme based on Double Chaining Algorithm	less complex and it needs small time for execution but the achieved security level is not satisfactory
Mathur et al. [72]	2016	Text Encryption based on AES where the dynamic key selection is present.	A satisfactory level of security is present though the volume of computation is high.
Sherkhane et al. [102]	2017	text encryption scheme based on Armstrong number and color code	Simple but less security level is provided by the scheme
Kumar R et al. [44]	2018	Text encryption scheme based on DNA ASCII table	High level of security but the volume of computation is extremely higher
Kottu et al. [94]	2018	Text encryption algorithm based on DNA sequence, prime number and PI sequence	High level of security but very complex and high computation cost
Muhammed et al. [65]	2019	Text encryption method based on random operation	Standard level of security is provided by this scheme but the complexity and computation cost is higher

2.6. Image Encryption

Zhou et al. [117] introduce an image encryption scheme based on a binary key image in 2009. The key image is generated from another image by considering the bit plane or the edge map from that image where its size is the same as the original image. Lossless image encryption is carried out between the original image and binary key image using a key image encryption technique. The security achieved by this scheme is not so much high.

Kaur et al. [91] represent an image encryption technique based on a scrambling scheme with key based technique. Multiple levels of Hash-based encryption are performed in this scheme. The scheme has several advantages. The scheme generates an encrypted image which contains very less amount of noise and different keys are applied for each time when encrypting the same image for multiple times. The security level achieved by this scheme is moderate as compared with existing schemes.

Pakshwar et al. [84] discuss a random scrambling based image encryption scheme with the help of XOR operation in 2013. The pixels of the original image are shuffled by using the scrambling technique and then it is divided into pixels blocks. Finally, the XOR operation is carried out for encrypting each of the blocks. The main restriction of this scheme is that it is only applicable to a grayscale image.

Verma et al. [111] represent a symmetric key based encryption scheme for multimedia files in 2014. In this approach, the symmetric key is generated randomly from the multimedia file based on special function. The scheme uses simple operations and generates a lossless encrypted multimedia file. The security level of this scheme is not so satisfactory though the speed of this scheme is very fast.

Madhu et al. [99] introduce image encryption schemes in 2014. In the first algorithm, encryption and decryption are carried out by key image with the help of XOR

operations. In the second algorithm, one of the bit planes from the key image is applied to encrypt the bit planes of the original image by applying XOR operation and shuffling is carried out to generate an encrypted image. The main limitation of this scheme is that the selection of proper key image determines the level of encryption.

Islam et al. [58] discuss a symmetric key encryption scheme in 2015 where an image is used as a secret key. The bits of the original message and key image are matched. When a match is found that location is kept in the ciphertext file. The receiver picks the location information from the image file by considering the location from the ciphertext. The main drawback of the scheme is that of ciphertext is shared without encryption.

Zhao et al. [107] represent an image encryption scheme in 2015 based on public key cryptography with phase retrieval algorithm where a fingerprint is used as a key. Encryption of this scheme is performed by the public key of RSA and fingerprint where decryption is carried out by the private key of RSA with the fingerprint. The scheme provides a standard level of security though the sharing of user private fingerprint image through the public network may reduce the acceptability of this scheme.

Yeole [6] proposes a multiple layer image encryption scheme based on the LSB data hiding method with XOR operation in 2016. In this scheme, the original image is encrypted by the XOR operation. Then stego image is generated from the encrypted image by applying LSB data hiding technique. Finally, the stego image is encrypted again. The security level provided by this scheme is not so high as compared with standard algorithms.

Khalaf [2] represents an image encryption method for color image based on random image key and XOR operation in 2016. The random key is generated from the image and XOR operation is performed between the bits of the original image and random

image key. The scheme provides a moderate level of security but the volume of computation is higher.

Dongare et al. [11] propose a key based image encryption scheme in 2017. In this scheme, three separate keys are generated from the red, green and blue color channel of the original image. XOR operation is performed between the keys and the binary values of the image pixel to generate the encrypted image. Security level provided by this scheme and quality of the encrypted image is not as high as compared with standard schemes.

Somaraj et al. [100] represent an image encryption scheme in 2017 based on the edge map of the key image with XOR operation. In this scheme, the edge map of key image is generated by applying gradient operators like Prewitt, Canny, Sobel and Roberts edge detectors. XOR operation is performed between the edge map and the original image to generate an encrypted image. Medium level of security is achieved by this scheme.

Bahumik et al. [32] introduced a new image encryption scheme based on the symmetric key. In this scheme, the original image is divided into 16 pixels blocks and again each block is permutated by applying the invertible linear transformation. Finally, XOR is performed between, permutated image pixel and bytes of the expanded key to generate the encrypted image. Moderate level of security is achieved by this scheme but the volume of computation is higher.

Table 2.4 represents the comparison between different image encryption schemes.

Table 2.4: Comparison of Different Image Encryption Schemes.

Authors	Year of Publications	Core Idea	Advantages & Limitations
Zhou et al. [117]	2009	Image encryption scheme based on binary key image	Simple & fast but less security level
Kaur et al. [91]	2012	Image encryption technique based on the scrambling scheme with key based technique	The security level achieved by this scheme is moderate but high level of computation is needed
Pakshwar et al. [84]	2013	Random scrambling based image encryption scheme with the help of XOR operation	Moderate level of security but this scheme is only applicable for grayscale image
Verma et al. [111]	2014	Random symmetric key based Image Encryption scheme	Easy to implement but security level is less
Madhu et al. [99]	2014	Image encryption based on bit planes of the key image with shuffling	Moderate level of security but the level of encryption is depended on selection of the proper key image.
Islam et al. [58]	2015	Symmetric image key based image encryption scheme	Moderate level of security but ciphertext is shared without encryption.
Zhao et al. [107]	2015	Image encryption based on public key cryptography with phase retrieval algorithm where a fingerprint is used as a key	Provides a standard level of security but the user has to share private fingerprint image through the public network

Yeole [6]	2016	Multiple layer image encryption schemes based on LSB data hiding method with XOR operation	Easy to implement but the security is not so high as compared with standard algorithms
Khalaf [2]	2016	Image encryption method for color image based on random image key and XOR operation	The scheme provides a moderate level of security but the volume computation is higher
Dongare et al. [11]	2017	Multiple key based image encryption	Simple and fast but Security level and quality of the encrypted image are not as high as compared with standard schemes
Somaraj et al. [100]	2017	Image encryption scheme based on edge map of the key image with XOR operation	Easy implementation but Medium levels of security is achieved by this scheme
Bahumik et al. [32]	2018	Image encryption scheme based on symmetric key, pixels blocks and invertible linear transformation	Moderate level of security is achieved by this scheme but the volume of computation is higher

2.7. Steganography

Karim et al. [88] represent a new image steganography scheme based on the Least Significant Bit (LSB) of an image and secret key in 2012. Image steganography approach is carried out in this scheme where secret information is embedded into different position of LSB of the image based on the secret key. LSB substitution

method is applied here. The limitation of this scheme is that using only LSB locations for hiding secret information reduces the security level.

Akhtar et al. [68] propose a new LSB based image steganography technique with the RC4 algorithm in 2013. In this technique, the bits of the original image are hidden in LSBs of cover image by following the sequences generated from the RC4 algorithm. After the embedding, some LSBs having a similar pattern to other bits are inverted to reduce the number of modified LSBs. This technique imposes more security over basic LSB based approach but a higher rate of computation is needed.

Xia et al. [121] discuss the detection scheme to attack for LSB matching steganography used for grayscale image in 2014. Low order differences of the histogram are estimated by Laplace distribution and features extraction is carried out by the co-occurrence matrix. Extracted features are supplied to support vector machine classifiers for identifying of test image that the image is original or stego image. The method is evaluated by LSB matching and applied to detect the attacks on LSB based steganography scheme.

Juneja et al. [55] represent a hybrid image steganography scheme based on LSB and AES techniques in 2014. In this technique, AES is applied to encrypt the secret information. Feature detection scheme combined with Canny and Hough transform is applied to detect the edge and smooth areas of an image and LSB Substitution and Adaptive LSB substitution are applied for edge and smooth areas for hiding the secret information. Though the scheme provides a considerable amount of security volume of computation is extremely high.

Singh et al. [4] represent a new steganography scheme based on LSB technique applied on planes of the color image in 2015. In this scheme secret information is hidden into three planes of RGB image. As multiple planes are used so embedding capacity and image quality are increased. The limitation of this scheme is that all the

hidden information is embedded into only LSB of the image so accessing only the LSBs may disclose the hidden information.

Majeed et al. [48] discuss an improved LSB and bit inversion method based steganography scheme for a color image in 2015. After embedding the secret information in LSB of the color image, LSB's of some pixels are inverted if some specific pattern of bits relating to the pixel is tracked. Thus less numbers of pixels are modified. Two levels of security are present here. In the first level, only blue and green color is used and the red color is considered as noise. Bit inversion techniques are done in second level. The scheme provides better security as compared with basic LSB scheme though computation cost and complexity is higher for this scheme.

Raju et al. [83] represents a modified LSB based image steganography scheme in 2015. In this scheme, some portion of secret information is embedded with LSB and another portion of secret information is embedded with some selective bits of cover image by applying a secret key. The key is generated from the image. The scheme provides a medium level of security as compared with basic LSB scheme as a combined approach is applied here.

Thenmozhi et al. [53] discuss a new LSB and Spiht based steganography scheme in 2016. In this scheme, the secret message is compressed by SPIHT method and then compressed information is embedded with LSB of a cover image. Compressed information is converted into binary blocks and then the sequence of the blocks is changed by applying key based random permutation. Finally, the information is embedded with LSB of the cover image. The security level provided by this scheme is not so satisfactory as compared with other LSB based schemes.

Katre et al. [14] propose an LSB based steganography scheme with the dynamic key in 2017. Dynamic key is generated by performing circular shifting and XOR operation on the image. Bits of the original image and dynamic key are XOR-ed to generate the encrypted image. LSBs of cover imaged are taken for merging the bits of

the encrypted image. Security level provided by the scheme is not so satisfactory as compared with other methods.

Cataltaş et al. [74] represent an image steganography scheme based on improved LSB based technique in 2017. In this method logistic map is applied to generate the random number. XOR is performed between the bits of a random number and original image to generate the encrypted image. The difference of values between LSBs of each pixel's RGB channel of the original and encrypted image are compared and balanced by improved LSB based scheme. This scheme provides better security as compared with basic LSB techniques.

Sarkar et al. [12] discuss a new LSB base steganography technique based on pixel selection in 2018. In this scheme, the middle region of the cover image is considered as the beginning pixel for hiding secret bits. Four diagonal pixels based on the middle region are considered for embedding the secret data in the next iteration. In this way, pixel selection is performed in quadrilateral direction and secret data is merged till the four corners of the image are reached. The scheme provides a medium level of security as compared with other LSB based techniques.

Rajput et al. [23] introduce a new LSB based image steganography technique based on Random insertion and Run Length encoding in 2018. In this scheme, Run Length encoding is carried out on a secret message where the RGB component is used to encode the secret message. Linear congruential generator (LCG) is performed for inserting the data in LSB of pixels in a random manner. At the time of data merging a 3R-3G-2B LSB pattern is followed. Though a considerable level of security is provided by the scheme high probability of image distortion is present in this technique.

Table 2.5 represents the comparison between different steganography schemes.

Table 2.5: Comparison between Different steganography Schemes

Authors	Year of Publications	Core Idea	Advantages & Limitations
Karim et al. [88]	2012	Image steganography scheme based on the Least Significant Bit (LSB) of an image and secret key	Simple and lower computation time but less level of security
Akhtar et al. [68]	2013	LSB based image steganography technique with RC4 algorithm and bit inversion technique	This technique imposes more security over basic LSB based approach but a higher rate of computation is needed.
Xia et al. [121]	2014	Detection scheme to attack for LSB matching steganography used for grayscale image	Moderate level of security but this scheme is only applicable for grayscale image
Juneja et al. [55]	2014	Hybrid image steganography scheme based on LSB and AES techniques	Scheme provides a considerable amount of security but the volume of computation is extremely high
Singh et al. [4]	2015	Image steganography scheme based on LSB technique applied on different planes of color image	Simple and less volume for computation but security level is less
Majeed et al. [48]	2015	improved LSB and bit inversion method based steganography scheme	The scheme provides better security as compared with basic LSB scheme though

			computation cost and complexity is higher for this scheme.
Raju et al. [83]	2015	LSB and key dependent selective bits based image steganography scheme	The scheme provides a medium level of security but complexity is higher
Thenmozhi et al. [53]	2016	LSB and Spiht based steganography	Easy to implement but the security is not so high as compared with standard algorithms
Katre et al. [14]	2017	LSB based steganography scheme with dynamic key	Fast but Security level provided by the scheme is not so satisfactory as compared with other methods.
Cataltaş et al. [74]	2017	image steganography scheme based on improved LSB technique with the logistic map generated random numbers	High security but Computation volume is higher
Sarkar et al. [12]	2018	LSB base steganography technique based on pixel selection method	The scheme provide a medium level of security but with less computation speed
Rajput et al. [23]	2018	LSB based image steganography technique based on Random insertion and Run Length encoding	Considerable level of security is provided by the scheme but high probability of image distortion is present in this technique

2.8. Conclusion

In this current chapter, a background study of image encryption, text encryption, user authentication and steganography are carried out. Different approaches from text, image and authentication domains which are developed earlier by various researchers are reviewed in this chapter. Emphasis is given on the specific areas of mentioned domain relating to current research interest.