CHAPTER 2
LITERATURE REVIEW

2.1 INTRODUCTION

The color visual cryptography techniques are liberated from the limitations of unpredictability on color images. The fundamental concept in visual cryptography is error diffusion and pixel synchronization. Error diffusion is a simple method performs filtering operation in eliminating the quantization error at each pixel level and offers the input to the next pixel. The error diffusion method results in low frequency between input and output image reducing the quality of image. The main advantage of pixel synchronization is avoidance of Degradation in colors.

A cryptographic technique is utilized to allow encrypted visual information. Correspondingly, decryption is carried out by the human visual system. The overall process of encryption and decryption is referred as Visual Cryptography Scheme. Most of the visual information is broadcast through the network in an easy way with a high speed due to increase in the technology of the network. But the security plays a significant responsibility in the visual information transmission process. To improve the security of the visual information, an efficient cryptographic technique is necessary to encrypt the image with malicious intentions during the time of image transmission. The encrypting systems of expected cryptography are generally used to preserve information security.

In data mining, Privacy preservation plays a vital role in facilitating an efficient communication for the users. Several methods are utilized for privacy preservation scheme like Secured Multiparty Computation, Data Transformation Technique and cryptographic Technique. Most of the present researches pay attention on SMC and DTT as the data mining sources are largely distributed in nature. But cryptographic techniques require more overhead for preserving privacy in distributed data mining context.

A secret image is enciphered with n number of shares and shared to n number of participants. The main objective of providing visual cryptography scheme is to obtain the secret image without in taking any cryptographic knowledge. Multiparty copyright protection scheme for highly secret color images is considered on preserving privacy by adapting the distributed key model. The unauthorized property of data and sharing control systems, breach their privacy. To address this
issue, a very efficient and robust visual cryptography scheme is required to enhance security to visual cryptography without occurrence of error. But the major complexity is a worst visual quality of the image which obtained during the distribution of image shares.

2.2 VISUAL CRYPTOGRAPHY FOR COLOR IMAGES

Visual cryptography is a technique of encrypting a Secret image into shares such that stacking a sufficient number of transparencies exposing the secret image. Transparencies are binary images generally delivered in shares. Each participant takes a share. Unlike conventional cryptographic methods, visual cryptography requires no difficult computation for achieving the secret. The task of decryption is to directly store shares and expose the secret image shares stored on the stacked.

The major disadvantage of the traditional visual cryptography scheme is share’s sizes are huge than the original secret image as each pixel of original secret image is converted into one 4 pixels block in share images. As a result the broadcasting requires high storage space and more bandwidth. In addition the encryption processes encrypt only one secret image reviewed survey of visual cryptography schemes [18] elaborately. The surveillance on visual cryptography shows different performance like pixel expansion, difference, safety measures, precision, computational difficulty, share created is purposeful or purposeless, kinds of secret images either binary or color and number of secret images either single or multiple encrypted.

Visual cryptography is the present area of research where lots of scopes are possible. At present specifically cryptographic method are used by different countries for secretly broadcasting text documents, economic documents, text images, internet voting etc. There are different modern concepts and additional methods occur for the basic visual cryptographic technique. One such enhancement is attempting to do. In the existing visual cryptographic schemes no security is offered to the secret shares and attackers modifies the bit sequences to generate fake shares. A better scheme against the vulnerability of the binary secret shares covered shares unnoticeably into some host images. During the decryption process, the secret shares are derived from the hidden images without requiring any of the hidden image properties as the watermark extraction technique [4], [63] is blind. The overlapping
of cover shares releases the original secret image. The decoded secret image quality is enhanced. But many possible improvements and additional techniques are required to improve further. The method is efficient but the cost increases in performing visual cryptography [62]. The initial model developed only for the bi-level or binary images or monochrome images.

The cost effective visual cryptography scheme [5], [68] appropriate for color image transmission over bandwidth constraint channels is demonstrated. In contrast to previously proposed schemes, the solution provides accurate reconstruction in generating shares with size smaller than that of the input image. A \( \{k, n\} \) visual secret sharing scheme based on MDS codes is presented which efficiently reconstruct the secret image.

A chromatic image is decomposed into three monochromatic images using HSV color model [67], [147]. Secondly, these three images are transformed into binary images by using cyclic shifting pixels technique. Finally, the traditional binary secret sharing scheme is used to get the sharing images. The scheme provides a more efficient way to hide natural images in different shares. Furthermore, the size of the shares does not vary when the number of colors appearing in the secret image differs and also identifies the cheater of shares.

### 2.2.1 Encryption of Image Shares

Information security turn into a most important challenge as information technology is revolving the world. Cryptography using mathematical methods is offering information security but needs difficult algorithms, intensive mathematical forecasts and better computational equipments. To keep away from such demanding and difficult algorithms, visual cryptography is elaborated which permits visual information like pictures, text, etc are encrypted in efficient manner. The decryption is operated by the human visual system, without any difficult cryptographic algorithms. VC technique encrypted an image into shares such that storing an adequate number of shares exposes the secret image.

In general access structure visual cryptography [132], [133] is better but the application runs good only for traditional black & white images and increases cost in color images. Visual cryptography encodes a secret image into \( n \) shares which are shared to \( n \) participants. Pixel Sieve method was proposed to encode an image into shares, but the encryption quality is poor. Enhanced the version of pixel sieve
method [6], [59] attain enhanced security then existing pixel sieve method. Depending on cross merge and key shifting schemes, the pixel sieve method creates quite noisy and extremely secure encrypted images.

The sound introduced by encoded secret pixels [2], [56] is completely diffused away to neighboring pixels and pleasing halftone shares are achieved. The secret image can be obviously decoded with no presentation any interference with the share image. An Extended Visual Cryptography Scheme (EVCS) [57] is a kind of VCS which consists of important shares to achieve good quality reconstructed image and to increase security with minimum pixel expansions.

The trend of pictographic data hiding is pixel based; here a version of visual cryptography [70] is presented which is segment-based instead of pixel based. The key or the covert which is in the outline of digits that is to be distributed is changed into segment display and then encrypted. The cross merge and key shifting schemes prevented the pixel increase in encrypted image and improved the security of the pixel sieve method. The enhanced pixel sieve method is widely used in a number of visual secret sharing applications which needs high quality secret images and high security such as electronic cash, secret maps etc.

The encryption of image offers better quality only in black and white image. But which provides better image encryption in color images with enhanced Visual Cryptography Scheme using Scrambling Pixels (VCSSP) [7]. Using the Arnold’s cat matrix, the pixels of the image is scrambled in a perfect way that margins of the secret image is not differentiated by storing shares and the attacker is attracted by examining more objects in the loaded image. Hierarchical decomposition of the RGB planes [72] of an image into equal-sized blocks is followed by an efficient shuffling of image blocks across the three color planes.

Most biometric systems suppose that the template in the system is protected due to human supervision or animal protection. Preserving the solitude of digital biometric data stored in a middle database has become a supreme importance. VCS [71] is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. A proper definition to the Visual Cryptograms of n (≥ 2) Random Grids (VCRG-n) [14], [85] for encrypting an image Particularly, a set of VCRG-n about image P comprising of n random grids written on shares such that only when the n shares are overlaid altogether in P, P is identified by human vision without any computing
device, as any group of less than n shares obtains no information about P. VCRG-n encryption schemes is designed for binary, gray-level and color images, authenticate the accuracy by formal proofs and reveal the possibility by computer simulations.

VCRG-n schemes do not needs any additional pixel expansion or any encoding basis matrix, which are required and expected in the techniques of conventional visual cryptography. Kafri and Keren’s random grid algorithm [86] and proposes an original algorithm to encrypt gray-level secret imagery in two ways. Numerous algorithms deal with text encryption. But, there are few researches done to date on encrypting digital images or video files. An improved way of encrypting digital images with password protection using 1D SHA2 algorithms [15] incorporated with a compound forward transform. A spatial mask is created from the frequency domain by intriguing benefit of the conjugate regularity of the composite imagery part of the Fourier Transform.

Spatial mask is then XOR with the bit stream of the innovative image. Exclusive OR (XOR), a logical symmetric operation, that produces 0 if both binary pixels are 0s or if both are 1s and 1 otherwise. XOR is confirmed just by modulus of pixel1, pixel2, 2. At last, confusion [87], [145] is performed depending upon the dislocation of the cipher’s pixels in step with a reference mask.

For creating uncertainty the image to be encrypted is wavelet transform is primary calculated and then rehabilitated into binary string and the hash of the secret key value (SHA1) [88] is in conclusion bit XOR to create the encrypted image. The experimental results, correlation examination of adjacent pixels of encrypted image in the horizontally, vertically and diagonally spaced pixels, histogram examination and Structural Similarity Index Measure (SSIM), tests have been approved out.

Nowadays, information security is gaining more attention in data storage and transmission. Images are broadly used in various processes. Consequently, the security of image data from illegal access is highly concentrated. Image encryption plays a vital role in the subject of information hiding. Image covering or encrypting techniques and algorithms range from simple spatial domain schemes to more difficult and dependable frequency domain ones.

A four level image encryption cryptography based on hash [9] that is, substituting a table for giving new values to the pixels. The central reason of this work is to support a method for protecting the images to the unrecognizable level
during transmission to stop the attacker. Multi level image cryptography is used based on chaotic system utilizes random integer function for the distribution phase but the algorithm provides large key space.

It integrates scrambling scheme with hash based methods which masks the image signal and make it more secure. The resulting system can securely encrypt the images for the purpose of storing images and transmitting them over the Internet. There are two major advantages associated with this system. The first advantage is that the encrypted image size is not very large because very little noise is added during encryption. The second advantage is that for every new image signal algorithm [75], [76] produces a new hash accordingly even a same image is encrypted double time the key is different in both times.

Visual cryptography methods encrypt the visual information such a way, that decryption is achieved by human visual system without any difficult decoding process. Visual cryptography is a secure strategy for broadcasting visual information but, if anyone gets access to all shares, the secret are revealed easily. A more impregnable visual cryptography scheme [10], [78] enciphers the secret using a symmetric key and then partitions the secret into shares. After storing of shares, the secret is hidden until it is not recognized. VC technique is apt for binary images. Here the symmetric key used for encipher and decipher is a small binary image. VC scheme is further improved for colored images and for covering multiple secrets. The symmetric key [77], [149] is less efficient so a better technique with stream cipher is required in improving the VC scheme. Encrypting information in transfer helps to secure it from hackers, because it is difficult to physically secure all access to network cannel. Standards cryptographic hardware and software are used to perform encryption and decryption.

2.2.2 Hiding Secret Shares

Visual cryptography aids cover a secret image into n number of shares shared to n number of participants. This kind of scheme is very purposeful as the participants in such security systems are unrecognized about cryptographic knowledge in order to get the secret image from the shares. This phenomenon is known as VCS. An Extended Visual Cryptography Scheme (EVCS) [8], [73] is the one which is proficient of producing significant shares compared with the shares of the VCS. EVCS by embedding the arbitrary shares result in VCS into hiding images.
General access structure is applied and each participant requires only one share to be transferred. The EVCS scheme is reliable and there are trade-offs between image visual quality and secret image pixel increase and between image visual quality and share pixel increase.

A visual cryptography scheme is a type of secret sharing technique which permits the enciphering of a secret image into shares distributed to participants. The attractiveness of such a VCS scheme is that a group of qualified participants is talented to reconstruct the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme is a type of VCS which employs purposeful shares compared to the arbitrary shares of traditional VCS. Technique named halftone visual cryptography [74] is implemented to achieve visual cryptography via half toning. It utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method.

A construction of EVCS which is understood by embedding arbitrary shares into purposeful hidden shares called Embedded Extended Visual Cryptography Scheme (EEVCS) [49]. In addition, it has many specific advantages against these well-known EVCSs, respectively. But expose some secret information by storing less than k shares together. The limitation of EVCS [12], [79] is overcome with the establishment of Embedded. Embedded EVCS is constructed by attaching arbitrary shares of secret image into significant hidden images. The embedded EVCS system is better with color images which is not possible in EVCS approach. Embedded EVCS approach tests the same algorithm for color images with respect to R, G, B values individually and appends shares to algorithm.

Embedded EVCS enhance the brightness of the reconstructed secret image and generates clear output image. The limitation is the method fails if high generation of (n, n) secret sharing scheme is provided. So a (n, n) secret sharing scheme [80], [82] is needed using multiple secrets. Presents a system that takes the four pictures as an input form and generates three images correspond to three of the four input pictures.

The disadvantage of embedded EVCS [13] is overcome in multi secret sharing scheme for encrypting two secret images into two shares. Multi secret
sharing schemes [83] transmit the two secret images with the use of two shares. With storing two shares, initial secret image reveal and with storing one of the shares with 90 degrees rotation in clockwise on other share exposes the next secret image. Distribute the distortion over two restored secret images. Moreover, the algorithms [84] can achieve no distortion.

In addition to (n, n) secret distribution, the (t, n) visual cryptography [16], [89] is a secret sharing scheme is also elaborated where a secret image is enciphered into shares, and the storing of any out of shares exposes the secret image. The storing of or fewer shares is not capable to derive any data about the secret. To reduce the overhead for producing and sharing transparencies in user changes, a visual cryptographic scheme with unlimited based on the probabilistic model. The VC scheme permits dynamic changes according to fresh shares without reproducing and redistributing the original shares. Particularly, an extended VC scheme based on source matrices and a probabilistic model is presented. Visual Cryptography [81] is an extraordinary encryption method to cover data in images in such a way that it is decrypted by the human visual system. The advantage of the visual secret sharing scheme is in its decryption tasks without any difficult cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique requires cryptographic measures to partition the image into a number of parts let n. k-n secret sharing scheme is a unique type of Visual Cryptographic technique where at least a set of k transparencies out of n shares exposes the secret data, less of hides information.

K-n secret sharing scheme [11], [66] is used for color image where encryption partition of the image is carried out using random number generator. But the main limitation of the algorithm is, it takes huge number of loops. Performs color visual cryptography using wavelet technique. Wavelet technique [64], [65] is used to convert the Color Image to Gray Image. The important feature of the Visual Cryptography is decryption doesn’t require any computer and it requires less computational power. An optical experimental technique [20] based on dynamic visual cryptography for the optical Control of vibration generation resources. A secret image is embedded into a stochastic background with the aid of initial stochastic phase deflection and phase identical algorithms.

The embedded image is interfered by a naked eye when the structure vibrates in the pre-determined rule. The decoding of the image is depending upon the
configuration of moiré fringes in the time-averaged image. A straightforward visual inspection [51] is sufficient to decide if the amplitude of vibrations is kept in the accepted range. The embedded image results in noise. A blind noise level decision happens in many image processing applications, such as de noising, compression, and segmentation.

Dynamic Visual Cryptography Scheme (DVCS) [19] based on chaotic oscillations has special computational algorithms which are needed for covering the secret image in the hidden moiré grating, but the decryption of the secret is totally visual. The secret image is revealed in the form of time-averaged geometric moiré fringes when the cover image is swigged by a chaotic law. The association among the standard deviation of the stochastic time variable, the pitch of the moiré grating and the pixel size promises visual decryption of the secret is extracted. The pseudorandom sequences generated by the two maps [95] are characterized by independence of their states, uniformly distributed, so hear integration provides excellent properties of confusion and diffusion, and an important space for the secret key. Certified Authority (CA) [94] that takes advantage of chaos to encrypt in a “unpredictable” manner, this provides a very attractive alternative method as there exists CA rules with chaotic behavior that, employed as pseudo-random number generators.

The metrics of these chaotic oscillations [50] is suspiciously preselected before the secret image is revealed from the hidden image. Binary compressed imaging. Compressed sensing and substantially minimizes the number of samples needed for conventional signal acquisition, at the cost of an extra reconstruction process. But the compressed image results in less image quality. JPEG2000 compliant coding scheme [52] successfully yields compressed images, with better quality indistinguishable to those of the original images.

A color visual cryptography encryption method that generates improved color shares through Visual Information Pixel (VIP) synchronization and error diffusion half toning [1], [17]. VIP synchronization sustains the location of pixels holding visual information of original shares throughout the color channels and error diffusion produces shares enjoyable to human eyes. Using CRC algorithm and Color VC scheme and error diffusion method [91], [92] generates the quality shares and diffuses the errors and provides the security from threat. VIP carries visual information of original image and VIP synchronization helps to keep the same
position of pixels throughout the color channels. Error diffusion generates shares which are clear and visible to human eyes and it improves the visibility of shares. VC schemes, [55], [90] however, they are not enough to be practical straight to color shares due to dissimilar color structures. Some methods for color visual cryptography are not acceptable in terms of producing either worthless shares or consequential shares with low visual quality, leading to suspicion of encryption. Color visual cryptography encrypts a color secret message into n color halftone image shares. Previous methods in the literature show good results for black and white or gray scale visual cryptography schemes, however, they are not sufficient to be applied directly to color shares due to different color structures. Digital Watermarking [53], [54] is used to recover the excellence and size of images obtains using color error diffusion technique. Secret information can be retrieve by stacking any k number of decrypted shares. A faster and easier color visual cryptography encryption method produces meaningful color shares via error diffusion halftoning. An error diffusion technique [93], [146] for halftoning produces shares which are more pleasant to human eyes.

Even Watermarking [124] is one of the attractive techniques which look after the copyright possession of a digital image. According to the proposed method, the watermark pattern does not have to be entrenched into the unique picture directly, which makes it harder to notice or recover from the marked image in a prohibited way. It can be retrieved from the marked image without making comparison with the unique image.

On the background of Visual cryptography, dividing the access structure maximizes Average Pixel Expansion (APE) where each of the participants takes multiple share images with various pixel expansions. On sharing digital document, lapses increases on maintain the privacy of the owners among digital document consumers. Here the entity user sharing data get revealed on due course of sharing, as exposé of private information, resulting in minimized information correctness. A privacy preservation technique is needed to secure the image shares.

2.3 PRIVACY PRESERVATION

Maintaining the privacy of digital biometric data like face images stacked in a central repositories turn into a vital importance. The probability of utilizing visual cryptography for preserving privacy to biometric data like fingerprint
images, iris codes, and face images is high. In the case of faces, a private face image is halted into two host face images known as sheet that are loaded in two distinct repository servers such that the confidential image is exposed only when both sheets are simultaneously available. Similarly, the specific sheet images do not expose the individuality of the confidential image. A novel visual cryptography scheme [21] shares two binary secret images on two rectangular share images with no pixel expansion.

The main challenge to deal with it is all about data security in a distributed environment. The concept is to build a privacy preserving database [22], [98] where data sharing operations are updated, limited access and control the handling of shared data, rather presenting data to central system, and hence, the database supports data sharing and privacy of data. Achieved data confidentiality by keeping the harmonize relations unbroken in the distributed environment.

The portable capability can be incorporated with cloud computing services to give more secure and advanced services to the subscribers. At the same time privacy [99] is an important issue in the collaborative ubiquitous computing since solitude concerns may prevent the parties from straight sharing the data and several types of information about the data. An approach addressing [100] such requirements, based on the use of high-level identity frication policies expressed in terms of identity attributes, zero-knowledge proof protocols and semantic matching techniques.

The scheme allowed the data owner to entrust major computation exhaustive process to distributed servers without exposing data contents or user access license information. Cloud computing [96] provides a new model for IT service delivery and it typically involves over-a-network, on-demand, self-service access, which is dynamically scalable and elastic, utilizing pools of often virtualized resources making cloud computing the next big thing after internet. Novel solutions for APKS based on a recent cryptographic primitive, Hierarchical Predicate Encryption (HPE) [97] is demonstrated.

Administrations, such as public-funded medical research centers, share de-identified information on their consumers to openly access database to hold to authoritarian needs. Many databases are controlled by third-parties and it is often unrecognized about the records received from different enterprise symbolized to the
similar individual. Failure to determine these issue results in biased like double counting of similar records and underpowered like unassociated records of different data type investigations.

A protective multiparty computation protocol [23] that allows record joins through customer encrypted identifiers. The protocol is more practical than earlier secure join models in that data accessing requirements to communicate with the third party. Though strictly possible, the speed of the fundamental protocol scales relating to the number of records. The method introduced an additional version of proposed protocol in which data holders add k-anonymous features of their customer to their encrypted data submissions. These characteristics aid more efficient join computation, supporting a proper security that each record is connected to no less than k individuals in the union of all administration consumers. Beyond a hypothetical action of the problem, the method offers a wide experimental evaluation. Privacy-Preserving data mash up algorithm [101], [102] to securely integrate private data from different data providers.

Privacy risk is one of the main challenges in multihop wireless networks, where attacks such as traffic investigation and flow tracing are simply initiated by a malicious attacker due to the unprotected wireless medium. Network coding involves the possibility to spoil these attacks as the coding or mixing task is optimistic at intermediate nodes. But, the simple use of network coding cannot attain the objective once sufficient packets are gathered by the attacker. On the other hand, the coding or mixing feature prevents the feasibility of using the onion routing an existing privacy-preserving techniques.

A network coding based privacy-preserving scheme [25] against traffic analysis in multihop wireless networks. With homomorphic encryption on Global Encoding Vectors (GEVs), the scheme provides two important privacy-preserving properties, packet flow untraceability and data content privacy, for efficiently preventing the traffic analysis attacks. Additionally, the proposed scheme holds the arbitrary coding feature, and each target recovers the original packets by reversing the GEVs with a very high chance.

Theoretical analysis and simulative evaluation proved the validity and efficiency of the GEVs scheme. Traffic analysis presents a grave threat to wireless network privacy due to the unlock scenery of wireless medium. In Multi-hop Wireless Network (MWN), [104] the mobile nodes relay others’ packets for enable
new applications and enhancing the network deployment and presentation. PrivCode [105] is intelligent to supply muscular privacy protection for wireless networks as the mix system since of its intrinsic mixing feature, and moreover, it can bring about better network performance owing to the improvement of network coding.

Two attribute-oriented authentication and transmission schemes [24] are used for protective and privacy-preserving health information sharing in Health Social Networks (HSNs). HSN users are labeled with dignified attributes. The attribute-oriented authentication scheme allows each HSN user to create an attribute identity with responsive attributes are anonymized. By authorizing the attribute identity, other users are capable to recognize the attributes an HSN user has. Online Social Networks (OSN) [103] has accelerated the appearance of vast amounts of personal information on the Internet.

The attribute-oriented transmission scheme allows HSN user to encrypt about health information into a cipher text related with a customized access policy. The access policy is defined by a target set of attributes. Only users for satisfying the access policy are able to decrypt the cipher text. The two attribute-oriented authentication and transmission schemes effectively oppose various attacks like fake attack, attribute-trace attack, eavesdropping attack, and collusion attack through security analysis.

The trouble of usage limit refers to the restriction of the data after publication. Data publishing is becoming a very demanding issue due to the wide development of the number of users involved in content sharing. The issue is addressed with better solution by providing a trusted hardware environment for each user but unfortunately its highly expensive one. Online social networks [26], [107] addressed problem in a limited environment and for the specific picture sharing application. In previous OSNs, the proprietor of an uploaded picture access the content but other users in the same content is unable to set the rule.

DECENT, [106] is a structural design for OSNs that uses a distributed hash table to accumulate user data, and features cryptographic protections for discretion and integrity, as well as support for elastic attribute policies and fast revocation. DECENT ensures that neither data nor social associations are perceptible to unauthorized users and provides accessibility through replication and validation of updates.
Separate social networking content from all other functionality that OSNs [108] provide which decoupling users control with their own social information. Third parties should have access to it, or they even choose to supervise it themselves. Such elasticity healthier accommodates OSN users’ solitude needs and partiality. Geo-aware Social Networks (GeoSNs) [109] pose privacy threats beyond those found in location-based services. Content published in a GeoSN is often associated with references to multiple users, without the publisher being aware of the privacy preferences of those users.

The mechanism of decentralized peer-to-peer online social networks is restricting the association of an adequate number of lawful peers. The mechanism is operated well as all faces in pictures are automatically confused during upload to the system. Additionally the enforcement of the complicated operation is assured recognition to the fundamental privacy preserving multi-hop routing protocol. The leak of each face relies on the rules set by holder of the face and malicious users are unable to reveal the content even if they are allowed to view.

A standard sensor network application is to examine objects, comprising wildlife, vehicles and measures containing information about an object transmission. Many times, the object requires to be secured for protective reasons. But, an intruder recognizes message path and follows the message back to source by travelling in the reverse direction of the path.

Context-Aware Location Privacy (CALP) [114] approach takes advantage of the ability of sensor nodes to perceive the presence of a mobile adversary in their vicinity in order to transmit data packets in an additional energy-efficient and privacy-preserving method. In exacting be relevant the concept of CALP to the expansion of a shortest-path CALP routing algorithm. Exploited source location privacy [27], [110] based on the evaluation of intruder trace back time and build routing protocol for the purpose of sharing message contents to various routes. The routing scheme increased the intruder’s average trace back time and attained max–min trace back time with definite energy conditions. WRS is the practical privacy aware routing protocol. WRS expand to an excessive intruder model, which permits the intruder to organize an adversary sensor network to trace the message routing behavior. Accordingly, the intruder is confused with the arbitrary schedule scheme. The approximation algorithm highly reduced the message delivery time in routing.
An enhanced version of Quality Of Service (QOS) aware privacy preserving location monitoring [111] is to enhance its routine and can reduce energy consumption and communication cost at the same time as augment the accuracy of the collective locations minimize their monitored areas. Traffic patterns [112], [113] are disguised by introducing fake packets to the generated traffic of original data. Many anti traffic analysis strategies are proposed and implements with the objective of attaining traffic uniformity in network. But the inclusion of fake packets adds up communication overhead in the network as a whole.

Privacy-Preserving Data Publishing (PPDP) [118] provides methods and tools for publishing useful information while preserving data privacy. Lately, PPDP has received considerable concentration in investigate communities, and many approaches have been planned for dissimilar data publishing scenarios. An overview of distance measure techniques [116] for privacy preserving discuss the distance measure models, and the major achievement ways and the strategies of distance measure algorithms, and analyze their advantage and disadvantage.

Data publishing play a vital role against individual privacy. The possibility of attacks from various threats to the privacy of the published data is high as per background knowledge. The privacy threat [28], [115] is the Full Functional Dependency (FFD) that is used as part of attacker knowledge. The method presented the cross-attribute correlations by FFDs. Unfortunately, none of the anonymization principles such as k-anonymity; ℓ-diversity, etc. are inefficient against an FFD-based privacy attack. The formalized FFD-based privacy attack [117] defined the privacy model, (d, ℓ) inference, to combat the FD-based attack.

The privacy issues rise by LBS [119], [120] and the challenge of implementing privacy-preserving location conscious systems give a concise overview of positioning techniques used by Location Based Services (LBS) and novel concept of locanym, which communicate to a pseudonym linked to an exact location that could be used as a basis for mounting privacy-preserving LBS.

Today’s location-sensitive service depends on user’s mobile device to decide the current position. As a result the service permits malicious users to access a limited resource or offer bogus alibis by cheating on their position. To address this issue, An Privacy-Preserving LocAtion proof Updating System. APPLAUS [29] is co-located with Bluetooth allowing mobile devices to equally produce location authentication and send updates to a location proof server. Occasionally modified
pseudonyms are utilized by the mobile devices to secure source location privacy from each other, and from the un-trusted location proof server.

APPLAUS established a user-centric location privacy model for deciding distinct user’s location privacy levels and determine the time and location of the proof request. Between ranking-based and correlation clustering-based approach is presented for exception revealing in order to protect against conspiring attacks. APPLAUS is implemented with network infrastructure, and is simply installed in Bluetooth permitted mobile devices with minimum computation or power cost. A broad experimental evaluation results proved that APPLAUS is able to effectively provide location proofs authentication, extensively maintain the source location privacy, and successfully detect colluding attacks.

AASLTU helps you to locate the street view of the location. The works by using Global Positioning System (GPS) [121] will track and show the mobile in the map. The application has a web portal which will allocate credentials to every user.

2.3.1 Cache System

The development of networking along with cost reduces in hardware resulting in a better implementation of distributed computing. The challenge arises in establishing proficient software for distributed systems and at the same time managing the difficulties. For instance, the fundamental hardware frequently facilitates interaction between devices with the help of network packets. Accordingly, developers of distributed applications necessity motive about communication patterns, write code to move and explore possibly difficult data structures into messages, write message code to path these messages from producers to consumers, and write code to unrevealed these messages back into data structures.

Researchers developed software distributed shared memories to support developers with the delusion of an easy shared memory concept on distributed systems. A direct execution of a distributed shared memory offers developers with an easy memory model to program. But, accessing far data in such execution needs time break for network communication and in addition is expensive. In reaction to this Issue, researchers urbanized distributed shared memory systems that attain better performance by relaxing memory consistency assurances. Rising software for relaxed memory consistency models is challenging as the developer reads and
recognize difficult memory consistency characters to recognize the likely activities of the program.

A distributed transactional memory system [35], [135] effort a chance to automatically hide network latency by hypothetically pre fetching and caching objects. The systems comprise an object caching framework, language additions to facilitate approach, and representative pre fetches. The pre fetching approach efficiently pre fetches objects without the computation or prediction of the addresses. Pre fetching approach provides violent use of both pre fetching and caching of isolated objects to cover network latency depending on the transaction entrust mechanism to maintain the simple transactional reliability model.

2.4 SECRET IMAGE SHARING

A secret image is tagged on documents, text files, manuscripts, photographs, pictures, and so on. With the idea of a secret sharing scheme, a secret image is encrypted into multiple component share images, and is then copied to shares. An extended VCS is capable of producing clear shares unlike the shares of the VCS. Constructed EVCS [33], [129] embed the arbitrary shares according to VCS into hiding images. But the secret sharing of the images are inefficient.

A number of participants are each offered with one of the shared images. When the participants store each of their shared transparencies upon each other, the secret image turns into perceptible. The process is termed as Visual Secret Sharing (VSS) scheme. As the decryption process does not depends upon any arithmetical computations, this cryptographic approach is achieved well without the use of computational devices. Conventional VSS schemes [128], [143] show performance issues about pixel expansion and contrast loss.

Conventional visual secret sharing schemes are built for a single secret image so it is ineffective to produce several share images for multiple secret images at a time. As a result, a visual secret sharing scheme for multiple secret images [34] is demonstrated. In the encryption process, [131] a storing correlation graph of secret pixels and share blocks is produced to denote the encryption functions, and a group of visual patterns is elaborated to generate two share images with respect to this graph. NxN watermark image to be embedded into an nxn secret image to build two shadows and then to be used to confirm the correctness of the reconstructed image. Checking to decide the dependability of all shadows before they are used to get
better the secret image prevents a contributor from incidentally or intentionally as long as unacceptable data.

Depending upon the loading characteristics of these patterns, the secret image is achieved from the two share images at aliquot stacking angles. Visual cryptography scheme generate ‘n’ number of transparent shares with reduced size and supports a variety of image formats and presents an integrated approach for binary, Gray and color image visual cryptography [130] by maintaining the visual quality and pixel expansion.

The major idea of the original visual secret sharing scheme [30], [123] is to encrypt a secret image into n purposeful share images. VSS unexposed any information of the shared secret by any grouping of the n share images except all images. The shared secret image is leaked by printing the share images on transparencies and storing the shares straightforwardly, so that the human visual system is able to identify the shared secret image without the help of devices. The visual secret sharing for multiple secrets VSSM permits the encryption of a larger number of secret images into a provided image area. The majority of VSSM schemes reduce the brightness of recover images as the amount of secret image encryption grows. These disadvantages restrict applicability of the VSSM schemes. The algorithm takes a hybrid encryption approach that includes a VC-based encryption and a camouflaging process.

The visual secrets sharing scheme for multiple secrets called VSSM scheme [122] encrypted more than one secret image into the same quantity of share images and maximized the encryption capacity in contrast to the original VSS scheme. But, the presented VSSM scheme uses a pre-defined pattern book with pixel expansion to encoded secret images into share images. Normally, VSSM results in at least 2× time’s pixel expansion on the share images. Therefore, the pixel expansion difficulty turns into more serious issue for sharing multiple secrets. The process maximizes the efficiency in sharing number of secret images.

Additionally, VSSM scheme [32], [127] is capable of sharing two binary secret images on two rectangular share images with no pixel expansion. The experimental results proved the better performance of VSSM approach not only in terms of no pixel expansion, but also in an outstanding recovery quality for the secret images.
Enhanced VSSM approach is the method that shares multiple visual secret images without pixel expansion. In addition, Secure Color Visual Secret Sharing Scheme Using Shifting Coefficient with no Pixel Expansion [37], [139] is used. The method introduced shifting coefficient value for the purpose of shifting the second share image to definite part. The shifting coefficient performs as a key in-between the participant without the additional confidential image leakage. The method supports better level of security also no pixel value are been expanded throughout the process. VSSM is enhanced with the development of Verifiable Multi-Secret Sharing schemes (VMSS) in terms of verifying the multiple secret shares.

In VMSS schemes, many secrets are shared but only one share is hold by each user and this share is verifiable by others. Two secure, efficient, and verifiable (t, n) multi-secret sharing schemes namely Scheme-I and Scheme-II, where Scheme-I depends on the Lagrange interpolating polynomial and the LFSR-based public key cryptosystem. The Lagrange interpolating polynomial [40] is utilized to partition and rebuild the secrets. The LFSR-based public key cryptosystem is engaged to verify the authority of the data. Scheme-II is designed with respect to the LFSR sequence and the LFSR-based public key cryptosystem.

Visual cryptography is one category of image encrypting. As visual cryptography is unlike from traditional cryptography, it does not require difficult computation to decrypt. Most of visual cryptography embedded with a secret is encoded using two shares limits. Numerous secret sharing schemes for digital images are developed in recent years. Traditional schemes generally dealt with the difficulty of computational complexity, and other visual secret sharing schemes arise with a higher transmission cost and storage cost. That is, each shadow size is m times as big as the original secret image. The (2,n) secret sharing scheme [31], [125] for grayscale images proposed is based a grouping of extracted image quality using Block Truncation Coding (BTC), high compression ratio Discrete Wavelet Transform (DWT) and high-quality biased performance of the Vector Quantization (VQ) technique. Non-expanded block-based progressive visual secret sharing scheme [126] with noise-like and meaningful shares, respectively demonstrate the feasibility of scheme.

It enables to share images without pixel expansion [137] and to detect a forgery as the color of the message is kept secret. Based on generalized random
grids, discussed two visual cryptography methods indicated as (2, n) GRG and (2, infinity) GRG. The (2, n) GRG is appropriate for the pre-determined number of shares, and the (2, infinity) method [36] is appropriate for the modifiable number of shares. The (2, n) GRG obtains better brightness on the stored result, and the (2, infinity) GRG allows expanding number of shares anytime. Multiple watermarks [136], [138] are normally providing extra security to an image by embedding two or more secret messages into the cover image.

An image sharing algorithm is based on the Discrete Fractional Random Transform (DFRNT) [39], [141]. The secret image is distributed into various shadow images in DFRNT domain together with a little number of noise images as the encryption keys to maximize the security. The decryption only needs apart of shadow images and so is autonomous of those noise images. The (t, n) threshold sharing scheme is executed totally by the defined algorithm.

K-threshold computational secret sharing technique [38] is that shares a secret $S$ into transparencies of size $|s|/k - 1$, where $|s|$ indicates the secret size. This combination is secure to the space optimal bound of $|s|/K$ as the secret is reconstructed from $k$ shares. In other words, k-threshold computational secret sharing technique is appeared as information dispersal scheme that offers optimal space efficiency. The scheme operates frequent polynomial interpolation and involves possible applications in secure information dispersal on the Web and in sensor networks. The Multiple-Parameter Fractional Fourier Transforms (MPFFT), [140] which can all right switch over information with no precede allotment of whichever secret keys or public keys between users.

A polynomial-based (k, n) Steganography and Authenticated Image Sharing (SAIS) scheme [41] was proposed to share a secret image into n stego-images. Simultaneously, a secret image is reconstructed with any k or more than k stego-images. But not possible to obtain any information regarding the secret shares from fewer than k stego-images. The attractiveness of a (k, n)-SAIS scheme is that it supports the threshold property and authentication. The threshold property with k as the threshold value, the steganography with stego-images looks like cover images and authentication indicating detection of manipulated stego-images.

All SAIS schemes require parity bits for authentication. An improved approach without needing parity bits (k, n)-SAIS scheme [42], [144] offers better visual quality and has higher detection ratio with respect to all previous (k, n)-SAIS
schemes. A common disadvantage of image sharing with steganography approaches is that the exposed secret image is imprecise due to the truncation of the grayscale secret image. To losslessly leak the secret image in the (t, n) - threshold, provided a better sharing scheme. In addition, the source host image is recovered by the embedded shadow images. The scheme extracts the secret shadows and produces the meaningful shadow images with the Sudoku. The Sudoku grid is set to 16×16 and partitioned into sixteen 4×4 blocks.

Sudoku embedded $4^*(t-1)$ secret bits into each pixel couple of the host image. In addition, the embeddable secret capacity is enhanced with respect to the threshold $t$ in (t, n)-threshold sharing system. The experiments prove that the shadows are successfully hidden away in the host image with suitable quality. The misrepresentation of the embedded host pixels is restricted within range. Additionally, the scheme provides a large ability for embedded secret data. DNA sequencing, Sudoku solution matrix and (t, n)-threshold sharing system [3] are used. DNA sequencing [142] is used to stand for secret image by smallest amount no. of bits and Sudoku solution matrix represent the cover image.

A robust copyright protection scheme for digital image, [48], [150] where the watermark does not need to be embedded into the secured image but is used to produce a secret image and a public image by using the visual cryptography technique. Then the secret image is recorded to certified authority for further protection. A blind authentication method [58] based on the secret sharing technique with a data repair potential for grayscale document images through the use of the PNG image.

An authentication signal is produced for each block of a grayscale document image with the binarized block element and is broadcasted into various shares using the secret sharing scheme. The concerned metrics are perfectly chosen as many shares as possible are produced and embedded into an alpha channel plane. The alpha channel plane is then united with the unique grayscale image to structure a PNG image. During the embedding tasks, the computed share values are mapped into a choice of alpha channel values of about maximum value 255 to achieve a transparent stego-image with a cover effect. The secret sharing scheme [43], [59] is useful for reducing the risk of incidental partial data loss. For tampered block data repairing is applied by reverse Shamir scheme.
In the process of image authentication, an image block is tagged as corrupted if the verification signal computed from the current block content does not equal the extracted shares embedded in the alpha channel plane. Data repairing is applied to each corrupted block by a reverse secret share scheme after gathering two shares from untouched blocks. Excellent experimental results proved the effectiveness of the method for real applications.

2.5 SECURITY IN VISUAL CRYPTOGRAPHY

The practice of the internet for broadcasting multimedia content becomes very often medium for the swap of digital information almost in all administrations using the internet. Therefore secure data in transmission is more important and a secured network is needed in order to guarantee safety of responsive data. A four-share visual cryptography scheme for color images partitions a secret image into four shares, the black mask and the other three shares. It was maintained that without knowing the black mask, no information about the secret image is attained even if all other three shares are recognized.

It showed better specific two-color secret image shares but security cannot be guaranteed. The method showed that an intruder cooperate arbitrarily selected two-color secret image from any two of other three shares with probability 4/7. The benefit increases to 6/7 if all other three shares are identified. The technique proved that extended to compromising secret images with more than four colors.

2.6 APPLICATIONS OF VISUAL CRYPTOGRAPHIC SHARES

Visual cryptography encodes a secret among various shares and decodes the secret by monitoring the stored shares using human visual system. The process is simple still powerful mechanism for distributing images effectively. The method is efficient due to the popularity, portability and simple computation ability. During shares transmission through local networks, particularly among mobile devices using Bluetooth, a share with a smaller size is preferred in order to minimize the cost of transmission and the hazard of being interrupted.

The improved development in the use of transmission of multimedia medical contents over unsecured and open networks gives insecurity for secret patient information over these networks. Digital encryption of medical images before transmission and storage [148] is proposed as a way to successfully offer security of
patient information. Encryption before watermarking of these images is essential in order to guarantee detachment of information to illegal personnel with patient.

A visual cryptographic technique for encrypting medical images [44], [61] is done before transmission or staking of shares. This process makes images inaccessible by illegal personnel and also promises confidentiality. The task has complete use of an encryption technique based on pixel shuffling and a secret key produced from the image. An error correction-coding scheme [60], [151] is also used to create an appropriate shadow. The logo extracted from the half-toned host image identifies the cheating types.

Visual cryptography is a kind of cryptographic technique in which no cryptographic computation is required at the decryption end. A (2, n) visual cryptographic scheme [46] helpful in banking operations by survivor mode where n is the number of produced shares, from which n-1 is the number of account owners in an account and one share is reserved to the bank authority. The technique one account holder should stack his/her share with the share of the bank authority and the secret image for user authentication is leaked. The technique involves two consecutive pixels taken as the one time input for the share creation process. This technique produces shares with less space transparency and supports better security. The technique is also simple to execute compared to other techniques of visual cryptography. The method involves text or picture are fed as a digital image in the system as the input and the system produces ‘n’ (2≤n) numbers of different images called shares, appear like images of arbitrary noise. Among ‘n’ number of shares user has to store ‘k’ number of shares, where 2≤k≤n, to expose the secret image.

The proceeds in internet and databases application techniques lead to maximized exact for remote querying the databases. Access for certified users becomes ordinary, which leads to the difficulty of copyright protection of relational repositories. Copyright security of outsourced relational repositories is also a significant issue in today’s internet-based database applications and in many content sharing applications.

Watermarking is a class of information hiding techniques, is useful to recognize the sources of data. Illegal replication and sharing is detected. The watermarking technique usually depends upon the accessibility of a large noise domain within which the objects are changed as retaining its necessary properties.
Various applications of watermarking technique like Copyright Protection, Single Ownership and Joint Ownership. Tamper Detection and Recovery are explored. A fully fledged copyright protection technique [47] along with fingerprinting, joint ownership and several other features for relational database is expressed.

Preserving the privacy of digital biometric data like face images stacked in central repositories becomes a vital importance. The chance of using visual cryptography for maintain privacy to biometric data like fingerprint images, iris codes, and face images is high. As mentioned before a novel VCS scheme, [134] that shares of two binary secret images on two rectangular share images with no pixel expansion. In the case of faces, a private face image is halted into two host face images known as sheet that are loaded in two distinct repository servers such that the confidential image is exposed only when both sheets are simultaneously available. Similarly, the specific sheet images do not expose the individuality of the confidential image.

2.7 RESEARCH GAP

SMC deployed variants of shared sessions, automatic privacy rule generation and restricting the unauthentic data exchange among scrupulous participants. On the context of Visual cryptography, partitioning the access structure increases average pixel expansion where each of the participants may take multiple share images with different pixel expansions. On distributing digital document, lapses arise on preserving the privacy of the owners among digital document consumers. Here the individual user sharing data get exposed on due course of distribution, as disclosure of private information, which results in reduced information accuracy.

Moreover, due to the social networking become more prevalent, the distributed data and file sharing among peer groups of authenticated work rules needs to be highly preserved for its privacy operations. While deploying filtering mechanism, focus was on the pixels that have to be filtered while emphasize was not based on the presence of noise in the pixels which results in the increase in execution time. Extra overhead arises resulting in privacy being compromised while distributing the cache, index among peers. As individual peer utilize some cache
space by way of compromising privacy. The security of secret image is addressed only when the number of collected valid shadows or secret sharing key is less than ‘k’, where security is provided for secret image using only a permutation key PK, which are generated in a random manner.

### 2.8 CONTRIBUTION OF THE THESIS

This segment describes the overall contribution of all left behind chapters of the work as follows,

- The work presents an efficient color image visual cryptic filtering scheme to improve the image quality on restored original image from visual cryptic shares.
- The color image visual cryptic filtering scheme presents a deblurring effect on the non-uniform distribution of visual cryptic share pixels.
- Fourier transformation is formalized to normalize the unevenly transformed share pixels on the original restored image.
- Texture overlapping filter is utilized to decide which parts of the input image to patched into the output texture.
- The overlapping portion of the two or multiple visual cryptic shares is planned to filter out with homogeneity of pixel texture property on the restored original image.
- Distributed file sharing is made efficient with cache-cache mechanism to reduce the overhead on increasing file sizes.
- Privacy of file sharing is done with file block id relating to the participant id using binary trees.
- Group dynamics is handled effectively with distributed key exchange model, based on the principal operation of minimum spanning tree variants.
- Error Transmission technique is designed in such a way to provide security and improve the quality of the reconstructed image in visual cryptography.
- The error free transmission divides the error values and distribute over adjacent pixels.