REVIEW ON VARIOUS TECHNIQUES FOR SECURE IMAGE TRANSMISSION

[1]M.J. Bheda, [2]Prof.Amita Shah

[1]M.E. Student, [2]Assistant Professor,
[1,2]Department of Computer Engineering
[1,2]L.D. College of engineering, Ahmedabad-380015, India

Abstract: ***These days, the entire world will be digitalized in all the ways. Each Business units, government offices, and military fields, research associations are utilizing the digitized image as exchanging mode for each basic information. These images usually contain either confidential or private information. During image transmissions, these highly confidential data can be manipulated by an unintended or unauthorized person, thus leading to insecurity for its sender. Therefore, it is essential to secure image. To solve this problem, many techniques have been proposed, in which data hiding and image encryption are the two main security techniques. This paper, we discuss the basic image security techniques, like Steganography Based Approach, cryptographic Algorithm Based Approach, visual cryptography based approach. This paper gives the future extent of Image security.***

Index Terms - LSB steganography, visual cryptography method, DCT, Symmetric and Asymmetric algorithm, Image security.

I. INTRODUCTION

Currently, the internet has become an excellent distribution system all over the world and helps us to communicate from one end to another. In the case of transferring digital contents through a medium is very crucial, because contents may be duplicated and destroyed. Modification of contents is relatively easy and achieved by using several techniques. Images are the major digital contents used in different areas like medical imaging systems, research area, business area, military system database, and services, etc. The important images will be transferred over unsecured communication channel network. Therefore, it is necessary to secure the confidentiality of images by protecting sensitive information from an intruder. This can be achieved by converting the original image to other non-readable formats before sending it to the intended receiver by using many techniques like image encryption and visual cryptography which generates noise like shares of image or by using data hiding technique also known as steganography is one of the fields that deal in methods related information security and hide secret message and other information from the unauthorized user.

The advantage of the image is that it covers more multimedia data, and it needs protection [1]. The cryptography is a kind of image security technique; that offers the secure transmission and storage method for the image over the internet. Security is the major concern for any system to maintain the integrity, confidentiality and image authenticity[2]. In today's rapid growth of digital communication and electronic data exchange, many of us communicate in cyberspace without thinking about the security of the same. The need for exchanging a lot of our private information and secrets in cyberspace. In today's highly computerized and interconnected world, the security of digital image/video has become increasingly more significant in applications such as pay-per-view TV, confidential video conferencing, medical imaging and in industrial or military imaging systems, online transactions, passwords, digital signatures legal's, etc. These applications need to control access to images and provide the means to verify the integrity of images. In many cases, such information leakage seriously violates personal privacy, example: the malicious spread of photos in personal online albums or patients' medical diagnosis images, and furthermore it may cause uncountable losses for a company or a nation, e.g. a secret product design for a company or a governmental classified scanned document. However, such convenience could also be used by malicious/unauthorized users to spread the image information rapidly that it may cause uncountable losses for the owner. The steganography and encryption for an image is performed to achieve the secure image transmission over the internet. The primary intention of keeping images protected is to maintain confidentiality, integrity, and authenticity [1]. Many techniques are available for making images secure and one technique is encryption.

II. Image Application:

The recent feasibility of much computer-based technologies has brought multimedia data transformation over the internet. The multimedia data can be included with image or video or audio or graphical objects that contain much important information of organizations, governments, hospitals, military. Among the many multimedia, the data image is widely used for many aspects of military, hospital, etc.

III. The necessity for image security:

Today, various people utilize distinctive applications to image data transfer. By far most of the people use their images for various customers using the social application. The attack on these social applications can copy or hack the important data. For better usage of these applications, users are using it on their mobiles, tablets, etc. The protection against the hacking attacks on that web or available plans, there exists a distinctive data security framework for multimedia data. These present security frameworks are either using encryption or steganography, or the combination of both. There is diverse securable image encryption that can be especially for protection against the unauthorized access. An Image transferred over the internet having important data of military, security associations, social or adaptable applications. Hence the image security is necessary. The commonly used security mechanisms are cryptography, steganography etc.

The transfer of the image over the unsecured transmission channel will pose following attacks such as active and passive attacks.

Active attacks: This consists of few data stream modification or false data stream creation.

Passive attacks: This attack uses the data but not affect the system resources [5, 6].

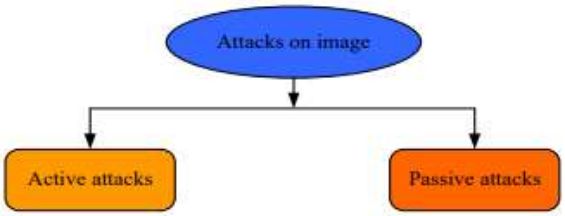

Figure.1 Attacks on image data

IV. Cryptography:

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in non-repudiation. This means that the sender and the delivery of a message can be verified. Cryptography is also known as cryptology[30].

Figure 2: cryptography

4.1 Different image encryption methods:

Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include[30]:

4.1.1 Secret Key Cryptography (SKC):

This kind of cryptography adopts the single key for encryption in which the sender can encrypt the message with this key and in receiving end the receiver will decrypt the message using the same key[8]. Examples: DES,AES,IDEA,TEA, Blowfish etc.

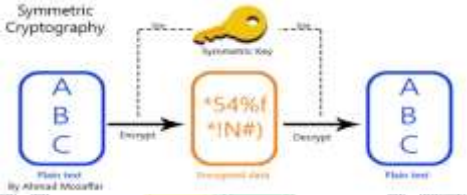

Figure 3: secret key cryptography

I. DES:

DES was developed as a standard for communications and data protection by an IBM research team, in response to a public request for proposals by the NBS - the National Bureau of Standards (which is now known as NIST). It takes an input block of 64 bit (8 pixels at a time) and applies Initial Permutation (IP) to it. The permutated data is then divided into two sub-blocks (Li, Ri). These sub-blocks after passing through sixteen round operations using different keys (48 bit) are finally permuted to obtain final ciphertext. The function block shown in DES is a combination of Expansion permutation (32–48 bit), Xoring Operation followed by substitution (48–32 bit) and final straight permutation box. The initial key length is 64 bits, out of which 8 bits are reserved for parity checks. Out of the remaining 64 bits, 56 bits are extracted using PC1. This 56-bit data is now divided into two halves and rotated various times to obtain 16 sub keys (56-bit keys). From these 56-bit subkeys, 48 bits keys (16 keys for round operations) are extracted using PC2. Decryption follows a similar mechanism of rounds as encryption does, but with the order of subkeys is inverted. Even though the encryption and decryption processes proceeds in a high number of rounds, the DES security mechanism is breakable in many ways. Brute force attack and known-plaintext attacks are the most common approaches [12]. Figure 4 shows the block diagram of DES. It shows how different subkeys are generated along with the encryption/decryption mechanism.

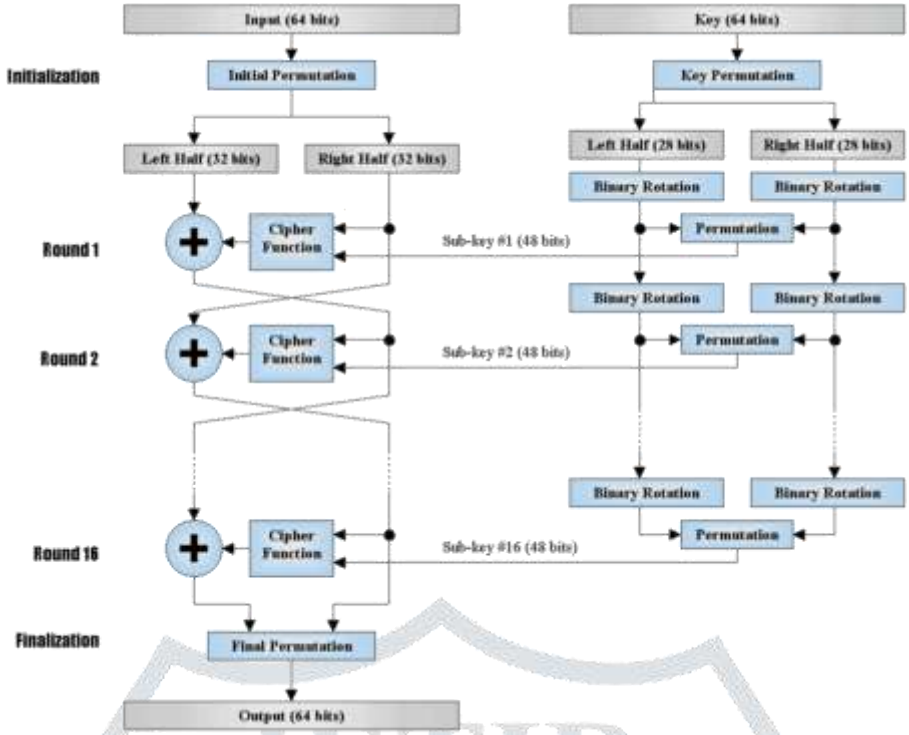

Figure 4: DES

II. AES:

Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register on December 2001 by the National Institute of Standards and Technology (NIST). AES is a non-Feistel cipher. AES encrypts data with a block size of 128-bits. It uses 10, 12, or 14 rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits as shown in figure 3. AES operates on a 4×4 column-major order matrix of bytes, known as the state.

Encryption Process:

Here, we restrict to a description of a typical round of AES encryption. Each round comprises four sub-processes. The first round process is depicted below −

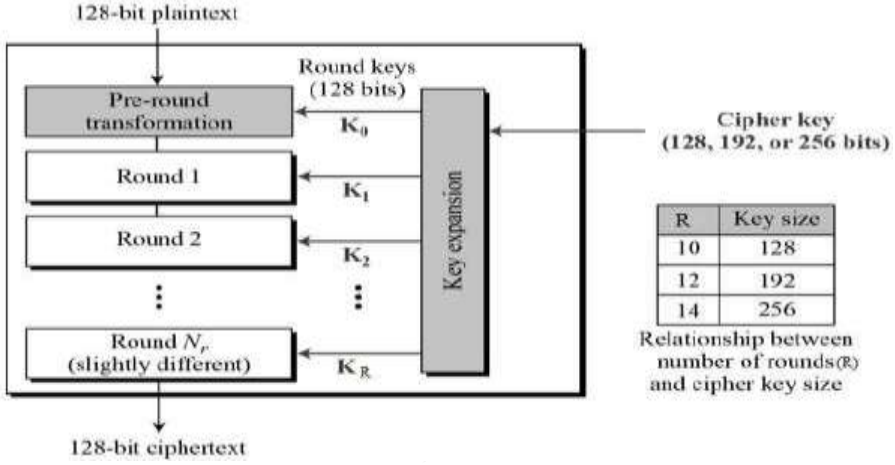

Figure 5: AES

Byte Substitution (Sub Bytes):

The 16 byte input are substituted by looking up a fixed table (S-box) given in design and the outcome is in a matrix of four rows and four columns.

Shift rows:

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of a row. A shift is carried out as follows −

- The first row is not shifted.
- The second row is shifted one (byte) position to the left.
- The third row is shifted two positions to the left.
- The fourth row is shifted three positions to the left.
- The outcome is a new matrix comprising of the same 16 bytes but shifted with respect to each other.

Mix Columns:

every column of four bytes is presently changed utilizing a special mathematical function. This function takes as input the four bytes of one column and yields four totally new bytes, which supplant the first section. The outcome is another new matrix comprising of16 new bytes. It should be noticed that this progression isn't performed in the last round.

Add round key:

The 16 bytes of the matrix are presently considered as 128 bits and are XORed to the 128 bits of the round key. In the event that this is the last round then the yield is the ciphertext. Something else, the subsequent 128 bits are translated as 16 bytes and we start another comparative round.

Decryption Process:

The procedure of unscrambling of an AES ciphertext is like the encryption procedure in the reverse request. Each round comprises of the four procedures directed in the reverse request −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in a reverse way, dissimilar for a Feistel Cipher, the encoding and decoding algorithms need to be independently implemented, in spite of the fact that they are immovably related.

A full brute force attack is the fastest documented attack and hence AES algorithms are comparatively secure.

III. Blowfish:

Blowfish is a symmetric-key block cipher algorithm. Its main component is a Feistel Network, iterating 16 times [12]. The size of the block used is same as DES algorithm (64 bits). But, unlike DES, it uses a variable key length of 32–448 bits. The block diagram shows that the 64-bit data (8 pixels) is divided into sub halves. These sub-blocks pass through 16 rounds of operation using S box, adder and bitwise Ex-or functions of the Feistel structure as shown in the Fig. 6. The output of each round is an input to the next round. Finally, the left and right sub-blocks are XORed with the key values (P ARRAY GENERATOR 17 and 18) and concatenated to obtain the final ciphertext. Blowfish uses a relatively large key: a P array containing 18 key (32-bit) numbers and four S boxes, each with 256 entries initialized to random values. The next step is to XOR P-array with the key bits, for example, P1 XOR (first 32 bits of a key), P2 XOR (second 32 bits of a key). In this way all-zero string is encrypted. This resultant output is now P1 and P2. This P1 and P2 are not encrypted with the modified subkeys to obtain P3 and P4. The process is repeated to obtain all the keys. Despite having a convoluted initialization, there is an efficient encryption of data.

Many of the Blowfish algorithms are still unbroken as those are protected by patent laws but Blowfish has its own limitations too. Its utilization is constrained to applications, like communication links, in which key changes infrequently. Also, as Blowfish has small block size, file greater than 4 Gb are not recommended to be encrypted.

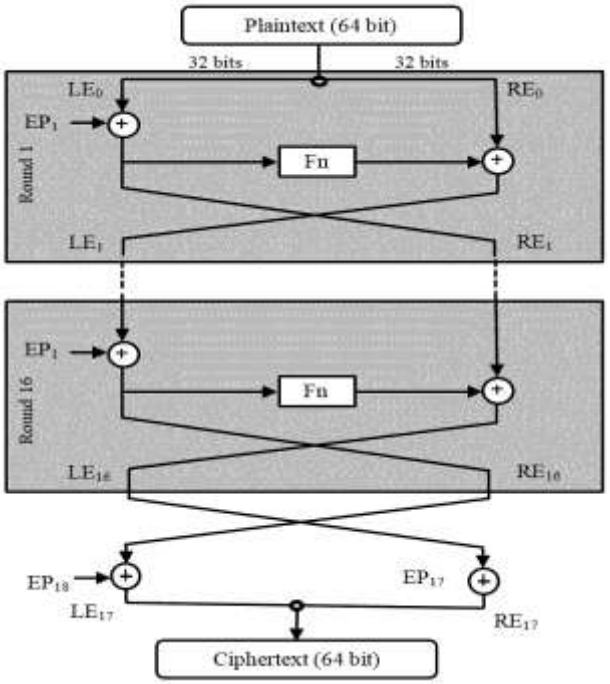

Figure 6: Blowfish

4.1.2 Public Key Cryptography (PKC):

The kind of cryptographic mechanism that contains two different types of key cryptosystems which are used to build a secure data communication among the sender and receiver over an unprotected network. In PKC a list of keys are used for encryption and hence it can also be considered as an Asymmetric cryptosystem. In this, there will be a public and private key that can be used for public and private communication.[8]. One key is the public key that anyone can access. The other key is the private key, and just the proprietor can get to it. The sender encrypts the information using the receiver's public key. The receiver decodes the information using his/her private key. For non-repudiation, the sender encrypts plain text employing a non-public key, whereas the receiver uses the sender's public key to decipher it. Thus, the receiver knows who sent it.

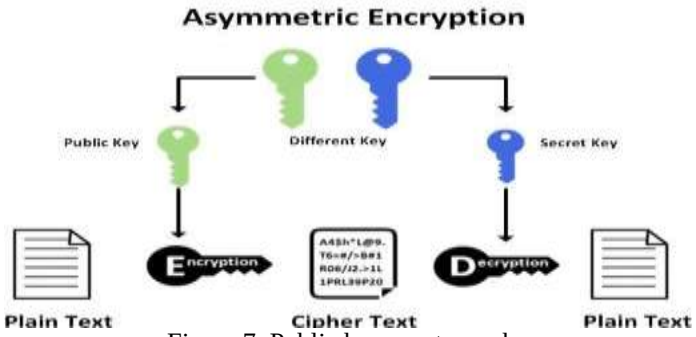

Figure 7: Public key cryptography

I. RSA:

RSA cryptosystem realizes the properties of the multiplicative Homomorphic encryption [13]. Ronald Rivest, Adi Shamir, and Leonard Adleman have invented the RSA algorithm and named after its inventors. RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. Let the plaintext is P and C is ciphertext, then at encryption, C = Pa mod n And at decryption side, P = Cb mod n. n is a very large number, created during the key generation process. The process is shown in figure 8.

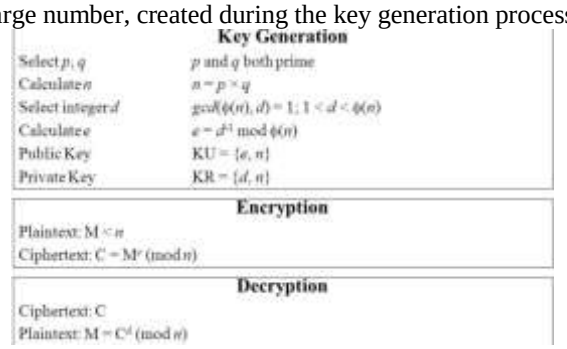

Figure 8: RSA

II. ECC:

Elliptic Curve Cryptography (ECC) is a cryptographic plan that uses the properties of the elliptic curve to create cryptographic calculations. In the 1980s Koblitz and Miller proposed utilizing the gathering focuses on elliptic curve cryptography. Over a limited field in discrete logarithmic cryptosystems. An elliptic curve is the arrangement set over a non-particular cubic polynomial mathematical statement with two questions over a field F. In short terms it is a discretized set of answers for a curve that is in the structure:

y2 = x3 + ax + b---------- (1)

If P1 and P2 are points which on the curve E, P3 = P1 + P2 Both clients consents to some publicly aware of information items.

1. The elliptic curve mathematical statement
2. Estimation of a and b
3. prime, p
4. The elliptical curve figure gathered from the elliptic curve equation
5. A base point, B, taken from the elliptic gathering.

Key generation:

1. A choose a whole number dA. this is A,,s private key.
2. A then produce a public key PA= dA*B
3. B correspondingly chooses a private key dB and process an public key PB= dB *B
4. A produces a security key K= dA *PB. B produces the security key K= dB *PA.

Signature Generation: For marking a message m by A, utilizing A,,s private key dA

1. Compute e=HASH (m), where HASH means cryptographic hash function, such as SHA-1
2. Select an arbitrary whole number k from [1, n − 1]
3. Compute r=x1(mod n), where(x1, y1) =k*B. If r=0, go to step 2
4. Computes=k−1(e+dAr)(mod n).Ifs=0,gotostep2
5. The signature is the couple of (r, s).
6. Send signature (r, s) to B client.

Encryption algorithm: Suppose A wants to send to B an encrypted message.

1. A takes plaintext message M and encodes it onto a point, PM, from the elliptic gathering.
2. A picks another arbitrary whole number, k from the interval [1, p-1]
3. The ciphertext is a couple of points.
4. PC = [(kB), (PM + kPB)]
5. Send cipher text PC to client B.

Decryption algorithm: Client B will take the following steps to decrypt ciphertext PC.

1. B computes the result of the principal point from PC and his private key, dB = dB * (kB)
2. B then takes this item and subtracts it from the second.

4.1.3 Hash Functions (HFs):

These are different from SKC and PKC. They use no key and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged. The image is also an important part of our information Therefore it's very important to protect our image from unauthorized access.Ex.MD5, SHA.

4.1.4 Performance evaluation:

Parameters	DES	3DES	AES	Blowfish	RSA	ECC
Cipher Type	Symmetric	Symmetric	Symmetric	Symmetric	Asymmetric	Asymmetric
Development	1970	1978	2001	1993	1978	1985
Key length	64	112,168	128,192, 256	Variable key length 32-448	Key length depends on no. of bits on a module	Smaller but effective key

Rounds	16	48	10,12,14	16	1	1
Block size (Bits)	64	64	128	64	Variable block size	Stream size is variable
Level of security	Adequate security	Adequate security	excellent security	highly secure	Good level of security	highly secure
Encryption Speed	Very slow	Very slow	Faster	Very fast	Average	Very fast

Table 1: Comparison of a various security algorithm

4.1.5 Encryption Time:

Comparison between symmetric and asymmetric algorithms such as between AES, RSA, and ECC are shown below. This compares the time taken to encrypt using these algorithms. This analysis shows that ECC is comparatively better than AES and RSA.

Key Size	Time Taken to encrypt in microsec		
	AES	RSA	ECC
6	1000	800	400
25	850	500	250
48	1100	720	300
102	2500	1200	650
128	250	120	70

Table 2 : Encryption time comparison [17]

V. Steganography:

Steganography replaces superfluous or unused bits in regular pc files (Graphics, sound, text) with bits of various and invisible data. Hidden information can be any other regular computer file or encrypted data[3]. According to Dictionary.com- "Steganography is hiding a secret message within a larger one in such a way that others cannot detect the presence or information of the hidden message". The Steganography term is springs from the Greek words "stego" implying "cover" and "grafia" implying "writing" and virtually means that "Cover writing".

The Steganography systems consist of the following elements:

1. Cover Object
2. The Secret Message
3. The Stego Object

1) **Cover Object:** In Steganography, the cover objects are those in which we hide a secret message. The cover object can be images, audio, videos, text. The most used cover object for hiding information is an image.

2) **Secret Message:** In Steganography, the secret message is the message to be hidden in a cover object. The secret message can be images, text messages etc.

3) **Stego Object:** The stego object is generated after hiding the secret message in a cover image. After that stego object is transmitted and then at receiver side processing is done on stego object to retrieve a message from it.

The secret message is embedded into a cover object using some embedding algorithms and it is extracted at the receiver side by reversing that procedure as shown in Fig.9. –

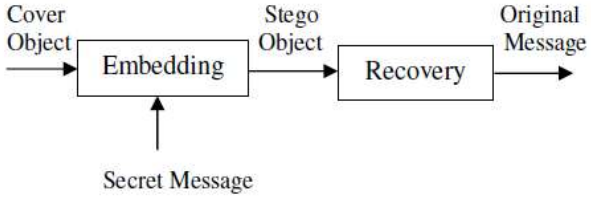

Figure 9: Block Diagram of Steganography

5.1 Types of Steganography:

A. Text Steganography

In text steganography, the text is used as a cover object. It hides a secret message behind the other text file. It is done by modifying the text or by modifying some features of text components. Different methods used are line-shift coding, word-shift coding, and feature coding. Text steganography was very much used in ancient times, but today these techniques have become obsolete. It is also known as linguistic steganography.

B. Image Steganography

In image steganography, images are used as a cover object. It hides secret messages into digital images. It makes use of the weakness of HVS as it cannot detect any variation in luminance part of color pixels. There are different algorithms for different file formats of images. These are the Least Significant Bit (LSB) insertion, Masking, and Filtering etc. JPEG, PNG, GIF (Graphics Interchange Format) etc. are the file formats for images which are used.

C. Audio Steganography

In this, a digitized audio signal is used for embedding secret message which produces modification of binary sequence order of the corresponding audio file. By inserting non-hearable tones in the audio signal used as a cover object data is embedded. Audio steganography exploits the weaknesses of the human auditory system (HAS). It exploits psychoacoustical masking phenomenon (makes a weak tone

unperceivable in the existence of a strong tone) of HAS. HAS cannot identify some variations in the sound waves. The methods used are LSB coding, Spread Spectrum, Echo hiding etc. MPEG, MP3 etc. are the file formats for audio which are used.

D. Video Steganography

In video steganography, the video is used as a cover object. Since videos are basically an aggregation of images and sounds, that is why many of the techniques can be implemented on video files also. The advantage of concealing secret information in the video is the fact that it is a moving flow of images and sounds and a large amount of information can be concealed inside a video. Any noticeable change might remain unobserved by humans because it is an uninterrupted flow of information. AVI (Audio Video Interleave), MPEG, and MP4 etc. are the file formats for video which are used.

E. Protocol Steganography

It is the process of hiding information network control protocols that are used in network transmission. It is also known as network steganography. Steganography can be used on the covert channels which exist in the OSI network model layers. Network protocols used are TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), and ICMP (Internet Control Message Protocol) etc.

The techniques including image steganography, audio steganography, video steganography, and protocol steganography are collectively known as technical steganography. Here, image steganography can be generally categorized into spatial domain and transform domain or frequency domain steganography.

5.1.1 Spatial Domain-based Steganography :

This technique involves the direct modification of the contents (pixel values) of the cover image to embed the secret message. Ease within the implementation and high embedding capability are the engaging options of this method. But this technique is less immune to image processing operations and susceptible to stego attacks. spatial domain steganography methods are LSB, pixel indicator technique etc.

LSB: In image steganography, almost all data hiding techniques try to alter insignificant information in the cover image. Least significant bit (LSB) insertion may be a common, straightforward approach to embedding data in a cover image.. For instance, a simple scheme proposed is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image. The altered image is called stego-image. Altering LSB does not modify the standard of an image to human perception however this theme is sensitive a range of image processing attacks like compression, cropping etc.[14]. LSB embedding is the easiest method in Steganography. It has high payload embedding capacity. Although it is less perceptible to the human eye, it is very prone to statistical analyses (Steganalysis detection)

5.1.2 Transform domain based Steganography:

A digital image consists of two types of frequency namely, high frequency and low frequency. Low frequency represents smooth and plane areas whereas edges are represented by high-frequency values. Unlike high-frequency regions, changes in the low-frequency regions are apparent to the Human Visual System (HVS) and there is a strong correlation among the pixel values of low-frequency regions [4]. Hence, regions of high frequency are preferable than that of the low frequency. In transform domain technique, the transformation of pixel values into the frequency coefficients is done using any of the transforms such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) etc. The secret information is then embedded into the coefficients. Transform domain methods are more immune to image processing operations, less susceptible to stego attacks and have lower data embedding capacity[4].

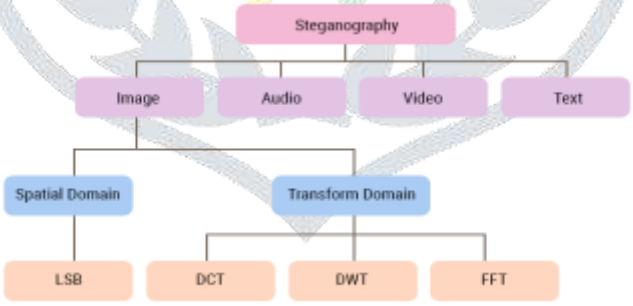

Figure 10: steganography classification

The Discrete Cosine Transform (DCT): This method is similar to the Discrete Fourier Transform. DCT transform the signal or image from a spatial domain to the frequency domain. The mathematical transforms convert the picture elements in such a way as to provide the impact of "spreading" the location of the pixel values over part of the image. The DCT is used in steganography as the Image is broken into 8×8 pixel blocks and transforms these pixel blocks into 64 DCT. Working from left to right, up to down, the DCT is applied to every block. Through a quantization table, each block is compressed to scale the DCT coefficients and message is embedded in DCT coefficients. The array of compressed blocks that represent the image is hold on in drastically reduced the quantity of space. When desired, an image is reconstructed through decompression, a process that uses the Inverse discrete cosine transform i.e. IDCT[15].

Discrete Wavelet Transform (DWT): It is used to transform the image from a spatial domain to the frequency domain. In the process of steganography, DWT identifies the high frequency and low-frequency information of each pixel of the image. It is a mathematical tool for decomposing an image hierarchically. It is mainly used for processing of non-stationary signals. The wavelet transform is based on small waves, Known as wavelets, of different frequency and limited duration. It provides both frequency and spatial description of the image. Wavelets are created by translations and dilations of a fixed function are known as mother wavelet. DWT performs in one dimension and in the two-dimensional plane. The DWT is the accurate model than the DFT or the DCT and it is a multi-resolution description of the image. The current image compression standard JPEG 2000 is based on the wavelet transforms [15].

VI. Visual cryptography:

Visual cryptography is proposed in 1994 by Naor and Shamir who introduced a simple but perfectly secure way that allows secret sharing without any complex cryptographic computation, which they termed as Visual Cryptography Scheme. Visual cryptography is the art of encrypting visual information like written text, images etc. The encryption takes place in such a way that no complex mathematical computations are required in order to decrypt the secret. The original information to be encrypted is called a secret. After encryption, ciphers are generated and referred to as shares. The part of the hidden secret is known as a share. The fundamental idea behind visual cryptography is to share the secret among a group of n participants. In order to share the secret, it is divided into n number of pieces called shares. These shares are distributed among the participants. To reveal the original secret, each participant provides his own share. The shares of visual Cryptography exist in their regular shape for the duration of transmission in sequence over the network. However, the directly third party cannot predict the secret information with only a single share.

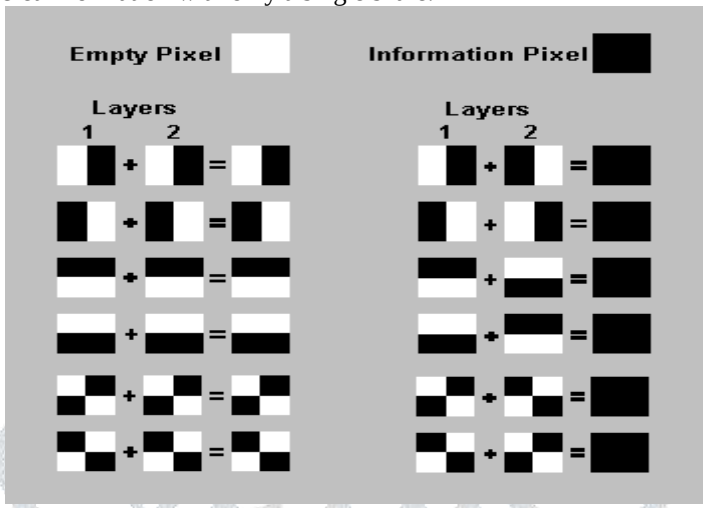

Figure 11: How Visual Cryptography works[8]

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal elements, there are white and two black blocks. In the table from above, we are able to see that a pixel, divided into 4 components, can have six special states. If a pixel on layer 1 has a given state, the pixel on layer 2 might also have one of two states: same or inverted to the pixel of layer 1. If the pixel of layer 2 is equal to layer 1, the overlayed pixel will be half of black and half white. Such overlaid pixel is called gray or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is contrary to the same pixel in layer 1. If both images are overlayed, the regions with identical states will appearance gray, and the areas with contrary states will be black.

The system of a pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

If the pixel states of layer 1 are absolutely (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a selected dispensed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers do not fall in the incorrect hands. When one in all each layers is intercepted it is not possible to retrieve the encrypted records.[8]

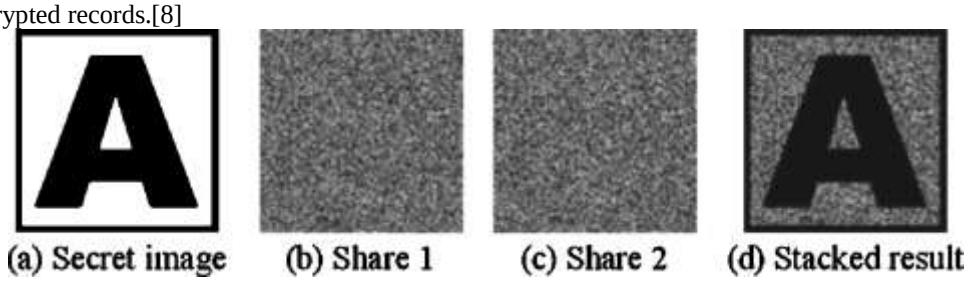

Figure 12: share generation

Types of visual cryptography:

1. Halftone visual cryptography–

A halftone image is made up of a chain of dots as oppesed continuous tone. These dots can be different sizes, exclusive colors, and sometimes even different shapes. Larger dots are used to represent darker, denser areas of the image, while smaller dots are used for lighter areas.

2. Color visual cryptography-

1) Color halftoning: we can do the color channel splitting first and then do the grayscale halftoning for each channel or we can do the color halftoning first followed by the splitting. 2) Creation of shares.

3. Visual Cryptography with Perfect Restoration[31]-

The half toning method degrades the quality of the original image. In this technique, both gray and color images are encoded without degradation. It retains the advantages of conventional visual cryptography. Here the stacking operation involves only XORing.

4. Multi-resolution Visual Cryptography[31]-

In traditional (k,n) visual cryptography, we only construct an image of single resolution if the threshold k number of shares are available. Progressive visual cryptography scheme in which we not only build the reconstructed image by stacking the threshold number of shares together but also utilize the other shares to enhance the resolution of the final image.

5. Progressive Multi resolution Visual Cryptography[31]-

In PMRVCS, the shares are ordered and merged in such a way that as more shares are used, the larger is the spatial resolution of the reconstructed image. A (n,n)-PMRVCS is defined as follows: Let I be the original image, S0, S1…Sn are the shares created. For k =1,2...,n-1, image Ik can be reconstructed by merging S0, S1…….Sk.

VII. LITERATURE REVIEW:

Security is a major concern for all the network environments. An image is one of the resources of sending information in all fields like medical image processing, networking, and in cloud environment also. There are many techniques for securing images. In this paper, a few of the prominent existing research work is reviewed to cover all the available image security techniques such as image Steganography, image encryption, and Visual cryptography.

1. Multiple layer text security using variable block size cryptography and image steganography

This paper [18] proposed a novel method which uses a variable block size symmetric algorithm which is content based. This algorithm includes binary XOR operation for encrypting the plain text and circular shift operation and folding method for making the key secure. Then, Raster scan and modified LSB steganography methods used to hide secret behind cover image, which gives good security to secret information. The experiments show that the encryption approach is able to fulfill the image encryption effectively through drawing the best parameters to achieve the best image encryption effect. For encrypted security, this proposed method has a strong sensitivity to the three digit key which may be break using the brute force method under different combinations of the key.

2. Advanced dual-layered Encryption for block-based Approach to Image Steganography

In [19] dual layer for the security of data is given, the first layer is done by encrypting data using the AES encryption algorithm and then encrypting the key used for the encryption using RSA. After that divide data in to ‘n’ block and embed them in ‘n’ images using LSB. Then further increasing the chaos factor by the random nature in which the image is sent. The three layers may increase the time for sending the data, however the time needed to decrypt the information increases potentially. The proposed method is much more efficient than the standard LSB method.

3. Visual cryptography for image depend on RSA & Elgamal Algorithms

This paper [23] introduced new visual cryptography for a color image by proposing a special table for both initial permutation and inverse initial permutation to increase the diffusion. Then dividing the plain image into blocks, each block represents share after applying the encryption algorithm on it such as RSA & Elgamal. The outcome of these operations is nine shares. Some encrypted with RSA and others encrypted with Elgamal, producing multiple shares in order to increase security for image during transferring it over the network.

4. Randomized visual secret sharing scheme for gray-scale and color images

In this paper[24] randomized visual secret sharing utilizes block-based progressive visual secret sharing and discrete cosine transform (DCT) based reversible data embedding technique to recover a secret image. The recovery method is based on progressive visual secret sharing, which recovers the secret image block by block. The proposed scheme achieves a contrast level of 70–90% for noise-like and 70–80% for meaningful shares. Experimental results showed that the proposed scheme restores the secret image with better visual quality in terms of human visual system based parameters.

5. New Watermark Embedding Technique using Visual cryptography

Author has proposed[21] progressive visual cryptography in which it creates n number of shares of a secret image. Progressive Visual Cryptography (PVC) means to progressively recover the secret image by superimposing the n shares of a particular secret image. The scheme structure is given for making n shares of any secret image. This scheme structure possibly gives sharing matrices which give the idea about how secret image can distribute among n shares. With the help of determination of various types of pixels the watermark embedding technique is implemented in this paper after finding the prediction error using those pixels. This visual cryptography scheme with watermark embedding technique works for both color and grayscale images.

6. Using Blowfish Encryption to Enhance Security Feature of an Image

In [20] dual layer for the security of data is given, the first layer is done by encrypting data using the Blowfish encryption algorithm and then encrypted data is divided into ‘n' blocks. After that o ‘n' block data is embedded them in ‘n' images using LSB. The proposed algorithm takes slightly more time to execute as three additional features are added to the algorithm namely: encryption using Blowfish algorithm, breaking of blocks and formation of a hash table. The proposed algorithm, since it uses more images, uses lesser data per image than the standard LSB and hence gives a higher PSNR value per image, which means the viewer will find it harder to differentiate even more than the standard LSB.

7. An efficient secure data transmission based on visual cryptography

In[27], the author uses a Tiny encryption algorithm to encrypt text and hide encrypted data behind images using LSB steganography method. For providing one more layer of security, visual cryptography is used, which generate shares of the secret image and then transmit these shares on an unsecured transmission channel. So, an intruder can not get any idea of secret from a single share.

8. A novel image encryption algorithm using AES and visual cryptography

Author[28] propose a secure image encryption algorithm that uses both AES and Visual Cryptographic techniques to protect the image. The image is encrypted using AES and an encoding schema has been proposed to convert the key into shares based on Visual Secret Sharing. if any intruder will be successful in getting the encrypted shares from the network, he or she cannot retrieve the original secret image without the availability of cipher. Also, the complexity of the encryption is double layered the hacker could not possibly get to know the algorithms used in the encryption. So it is still difficult to crack the visual cryptography even if the hacker gets his hands on the key shares over the network.

9. Security of Remote Voting System based on Visual Cryptography and SHA

In [26], the Proposed system does not use any biometric application, without using biometric function authentication of the voter is done. In this system, SHA2 is one of the strongest hash function technique which generate a 256-bit string of registered user data. This 256-bit string is then embedded into an image using the LSB data hiding technique. Two shares of this image are created using (2,2) visual cryptography algorithm. votes are encrypted by AES encryption algorithm to provide the security. AES encryption algorithm is faster so, encryption is done in minimum time. So, it saves time and improves the performance of the system. The proposed scheme is cost effective and at the same time satisfies the security requirements of an online voting system.

10. Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques

In [25], a novel approach is proposed for multimedia data security by integrating Steganography and Visual Cryptography (VC). The proposed method contains two phases. The first phase hides the message dynamically in a Cover Image1 by changing the number of bits hidden in RGB channels based on the indicator value. VC schemes conceal the Cover Image2 into two or more images which are called shares. In the second phase, two shares are created from a Cover Image2 and the stego image created in the first phase is hidden in these two shares. The shares are safe as they reveal nothing about the multimedia content. The Cover Image2, stego image, and the hidden message can be recovered from the shares without involving any complex computation. More amount of information can be transmitted by increasing the number of VC shares.

11. Color Image Visual Cryptography Scheme with Enhanced Security

In this paper[22], the author has proposed a highly secured visual cryptography scheme which uses AES encryption and error diffusion halftoning algorithms as intermediate steps in cryptography work. In the first step generate the shares of halftone images of each channel and then AES encryption is applied to preserve from the shares from malware activities which can modify the bit sequences to generate the unauthenticated shares.

12. A Hybrid Cryptosystem of Image and Text Files Using Blowfish and Diffie-Hellman Techniques

In [29], The proposed algorithm claims to be better than the existing algorithms since it takes the advantage of generating a variable length key using the Blowfish algorithm and at the same time work on its disadvantages. Blowfish can't provide authentication and non-repudiation. This drawback is taken care by Diffie Hellman shared key generation technique which ensures the file doesn't go to wrong hands while transferring it over a public network. The file is decrypted only if the key matches. Even if the file goes in wrong hands somehow, it will remain encrypted and not readable.

VIII. SUMMARY OF THE RECENT WORK:

Title	*Method used*	*Author remarks*	*Our findings*
Multiple layer text security using variable block size cryptography and image steganography (2017 IEEE) [18]	Variable size data encryption algorithm; Raster Scan LSB steganography method	1.Preserved the quality of stego image and cover image 2.Simple implementation and easy to recover data with LSB	1. Low data hiding and Same key lead the chance to attack while a transmission 2. Three digit Key size is very small n vulnerable to brute force attack.
New watermark embedding technique using visual cryptography(2017 IEEE)[21]	Progressive visual cryptography	1.High accuracy and PSNR rate 2.Less noise margin of an image	1.Require the large cover image to hide the data as shares increases, So increasing time complexity
Visual cryptography for image depend on RSA and Elgamal algorithms (2016 IEEE)[23]	Visual cryptography using IP table; Blocks encrypted using RSA and Elgamal	1.Provide the confidentiality and authentication of secret data/image 2. Diffusion is achieved very well	1. Work on small size data only and also increase time complexity 2. Pixel expansion give low-resolution image
Color Image Visual Cryptography Scheme with Enhanced Security(2017 springer)[22]	(2,2)halftone visual cryptography and AES	1. Perceiving any trace about the secret image from an individual share is difficult; also enhance the visual quality of an image	1. An algorithm uses the same key for encryption and decryption, this may lead the chance of attack while transferring the images and destroy the quality of the images

Multilevel multimedia security by integrating visual cryptography and steganography techniques (2016 Springer)[25]	LSB Steganography and Visual cryptography	1. Improve the quality of an image and a good approach for data security.	1.Low hiding capacity, vulnerable to steganalysis 2. Computational complexity is high.
Advanced Dual layered encryption for a Block-based approach to image steganography (2016 IEEE) [19]	AES, RSA and LSB steganography	1.high PSNR value .so less noise ratio; 2.Less complex structure	1. Require the more no. of cover images to hide the data as a size of data increases. 2.Vulnerable to steganalysis
Randomized visual secret sharing scheme for grey-scale and color images (2017 IET Journal)[24]	Randomised Visual Secret Sharing, DCT data hiding technique	1.Good PSNR value 2. high contrast and illumination achieved. 3. Achieved good color quality.	1. Blocking artifacts is the main problem in DCT which degrades visual quality of a reconstructed image.
Using Blowfish encryption to enhance the security feature of the image (2016 IEEE) [20]	Blowfish with LSB steganography	1. Increases the security factor of the image. 2. The encryption enhances the security and then the randomness increases	1. Require the more no. of cover images to hide the data as a size of data increases. 2.same key for encryption and decryption may lead the chance to attack and destroy the quality of the images
Security of remote voting system based on visual cryptography and SHA(2016 IEEE)[26]	SHA2 for creating a message digest LSB steganography AES	1.proposed scheme is cost effective and at the same time satisfies the security	1. AES works on symmetric key only.

IX. Conclusion:

Preserving image security has become a primary concern since transmission of images over the Internet channel occurs very frequently. In this paper, we have reviewed different image security techniques including image steganography, visual cryptography, and conventional image encryption technique. There are numerous image encryption techniques and each technique is unique in its own way. Particular image security technique provides good image quality at a receiver side, different embedding capacity while other provides degraded images; also certain image encryption techniques have less processing speed while other has high processing speed. In this paper, all of these properties of different image security techniques are reviewed and presented in tabular form. Other techniques of image security are also reviewed in this paper. Security is the major concern for any system to maintain the integrity, confidentiality and image authenticity. Although cryptography is an effective method it also faces the problem in providing the security if the data in the image is more. The study analysis of the existing research work helped in defining the research gap and providing the future research line for image security even better.

X. Acknowledgment:

I would like to thank my honourable teachers, fellow students, supportive friends and specially my family. I would also like to say thank to that person who guides me through the way, she continually and persuasively conveys a spirit of adventure in regards to my work Ms. Amita Shahmam.

XI. References:

[1] William Stallings, Cryptography and Network Security, Principles and Practice. Fifth edition.
[2] Artz, Donovan. "Digital steganography: hiding data within data." internet computing, IEEE 5.3 (2001): 75-80.
[3] https://www.ukessays.com/essays/computer-science/the-types-and-techniques-of-steganography-computer-science-essay.php
[4] Mansi S. Subhedara, Vijay H. Mankarb. Current status and key issues in image steganography: A survey. COMPUTER SCIENCE REVIEW 13–14 (2014) 95–113
[5] Hill, Douglas W., and James T. Lynn. "Adaptive system and method for responding to computer network security attacks." U.S. Patent No. 6,088,804. 11 Jul. 2000.
[6] Kaufman, Charlie, Radia Perlman, and Mike Speciner. Network security: private communication in a public world. Prentice Hall Press, 2002.
[7] Alfalou, Ayman, and C. Brosseau. "Optical image compression and encryption methods." Advances in Optics and Photonics 1.3 (2009): 589-636
[8] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm
[9] Kenneth H Rosen. Cryptography: theory and practice. CRC press, 2005.
[10] Denning, Dorothy E. "Cryptography and data security." (1982).
[11] Manju Kumari . Shailender Gupta. Pranshul Sardana; "A Survey of Image Encryption Algorithms", _ 3D Research Center, Kwangwoon University and Springer-Verlag GmbH Germany, part of Springer Nature 2017
[12] Matsui, M. (1994). The first experimental cryptanalysis of the Data Encryption Standard. Advances in cryptology—CRYPTO'94 (pp. 1–11). https://doi.org/10.1007/3-540-48658-5_1.
[13] Schneier, B. (1994). The Blowfish encryption algorithm. Dr. Dobb's Journal, 19, 38–40. http://www.drdobbs.com/security/the-blowfish-encryption-algorithm/184409216.
[14] Neeta, D., Snehal, K., & Jacobs, D. (2007). Implementation of LSB Steganography and Its Evaluation for Various Bits. 2006 1st International Conference on Digital Information Management.
[15] "A Survey on different techniques of steganography" Harpreet Kaur, Jyoti Rani, MATEC Web of Conferences DOI: 10.1051/matecconf/20165702003 ICAET 2016

[16] Naor, M., & Shamir, A. (1995). Visual cryptography. Lecture Notes in Computer Science, 1–12. doi:10.1007/bfb0053419
[17] A Arjuna Rao1, K Sujatha1, A Bhavana Deepthi1, L V Rajesh1 (2017), "Survey paper comparing ECC with RSA, AES and Blowfish Algorithms", International Journal on Recent and Innovation Trends in Computing and Communication, IJRITCC
[18] Shivani Chauhan, Jyotsna, Janamejaya Kumar, Amit doegar"Multiple layer Text security using Variable block size Cryptography and Image Steganography" 2017 International Conference on "Computational Intelligence and Communication Technology (IEEE-CICT).
[19] Shreyank N Gowda" Advanced Dual Layered Encryption for Block-Based Approach to Image Steganography" 2016 International Conference on Computing, Analytics and Security Trends (CAST) © 2016 IEEE
[20] Shreyank N Gowda " Using Blowfish Encryption to Enhance Security Feature of an Image" International Conference on Information Communication and Management © 2016 IEEE
[21] Swati Narkhede, Mahesh Shirole" New watermark embedding technique using visual cryptography" International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017) © 2017 IEEE
[22] Prachi Khokhar and Debasish Jena"Color Image Visual Cryptography Scheme with Enhanced Security" 2016 International Conference on Frontiers in Intelligent Computing: Theory and Applications © 2017 Springer
[23] Alaa kadhim, Rand Mahmoud Mohamed" Visual Cryptography For Image Depend on RSA & ElGamal Algorithms" International Conference on Multidisciplinary in IT and Communication Science and Applications © 2016 IEEE
[24] Nikhil C. Mhala, Rashid Jamal, Alwyn R. Pais "Randomised visual secret sharing scheme for grey-scale and color images" IET Image Process; The Institution of Engineering and Technology 2017© 2017 IET
[25]M. Mary Shanthi Rani, G. Germine Mary and K. Rosemary Euphrasia "Multilevel multimedia security by integrating visual cryptography and steganography techniques" 2016 cybersecurity and computational models, Advances in Intelligent © 2016 Springer
[26] Mrs. Nilam Kate, Mrs. J. V. Katti "Security of remote voting system based on visual cryptography and SHA" International Conference on Advances in Computing, Communications, and informatics © 2016 IEEE
[27] Rubeena Jabi, Punyaban Patel, Deepty Dubey, "An Efficient Secure Data Transmission Based on Visual Cryptography", IEEE International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016).
[28] Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandeeswari Loganathan, "A novel image encryption algorithm using AES and visual cryptography", International Conference on Next Generation Computing Technologies (NGCT-2016) IEEE.
[29] Tapan Kumar Hazra, Anisha Mahato, Arghyadeep Mandal, Ajoy Kumar Chakraborty," A Hybrid Cryptosystem of Image and Text Files Using Blowfish and Diffie-Hellman Techniques", IEEE 2017
[30] https://www.techopedia.com/definition/1770/cryptography
[31] https://www.slideshare.net/PratikshaPatil/visual-cryptography1