International Journal of Advanced Computational Engineering and Networking, ISSN(p): 2320-2106, ISSN(e): 2321-2063
Volume-9, Issue-1, Jan.-2021, http://iraj.in

SURVEY ON MULTIMEDIA SECURITY AND VISUAL CRYPTOGRAPHY

[1]ABHILASH S NATH, [2]A. JEYASEKAR

[1]Research Scholar, Dept. of Computer Science and Engg, SRMIST,KattankulathurCampus, Chennai 603203
[2]Associate Professor, Dept. of Computer Science and Engg, SRMIST, Kattankulathur Campus, Chennai 603203
E-mail: [1]abhilass@srmist.edu.in, [2]jeyaseka@srmist.edu.in

Abstract - The people using internet has become so extensive across different sectors in day to day life. Security is the important feature different across the platform and mobile applications we use. The important aspect in the sectors is usage of the data having significant role in identifying the user preferences in using the data for video, text and games etc. Due to the large volume of data consumed by the customers is high it's difficult for user to identify the identification of the pattern of data that is stored by the remote servers .The advertisements and the thumbnails that come across as your search relates can be seen. This understanding by the service providers or the sites that we visit store our preferences in choosing the content matters .Mostly people chooses the video content for news, entertainment .The people also uses camera for home security and even for live streaming personal mobile cameras used. These all uses huge amount of data. The information loss during the communication between the devices through internet there is a lack of features which even cannot be controlled by the protection software's. To avoid all leaky information from the transfer of data technique called visual cryptography is used. In this survey, present an overview of the characteristics, security threats and major security challenges. The contribution of the survey will lead to understand the visual cryptography and security facets of it. The various techniques existing in the visual cryptography will help to figure out the improvement of cryptographic technique in various years. Some identified areas of security which can also affect our day to day life which give motive to find new ways of security mechanism.

Keywords - Internet, Visual Cryptography, Information Loss

I. INTRODUCTION

The network is collection of interconnected devices. The network has been secured for large number of devices .There are different type of attacks which is happening in computer networks. The activity of hackers in to gain huge amount of information in multimedia data would generate a major concern for security. The multimedia applications created by the users find more vulnerable to different attacks. The major part of the idea is encryption of the large number of image shares. These attacks used efficient and secure way to break in to a system. While understanding the side channel attack by leaking information, the attacker can infer the activities based on size of the data of an encrypted video stream. The video market is expected to reach dollar 45 billion by 2020. Saving the bandwidth and space for storage a encoder removes spatial redundancy .Difference coding causes significant side-channel information leakage. Some of activities increase the storage space and increase the size of the traffic data. The visual cryptography increases the safety of the image in a huge way it help to store in a very important way it decreases the storage space of the data and increases the transmission of the data in a huge manner. Big Organizations wants strong security devices for analyzing the vulnerabilities in their networks. But with big scale networks and managing their complex configurations technically difficult.

The network has to be changed with configuration change in other networks. The network admin wants to respond newly invented weakness by giving new patches and changes to the network configuration or utilizing resources to reduce the risk from attacks.
Side-channel attacks gain technical information in the form power differential analysis and black-box attacks. The cases in the side-channel include cache attack, timing attack, power-monitoring attack and differential attack analysis.

II. TYPE OF SECURITY ATTACKS

In security attacks there are two type of attacks which are passive and active attacks. Passive attack means it make use of information without any need of algorithm. They learn the information but don't change the device operations. The main feature of passive attack is to monitor the operations. It just wants the information which is transferred. Release of message content and analysis of traffic which are types in passive attacks. Sensitive information collected through mail or talking through communication devices. The information received through email can identify by observing the pattern in which the length of messages and location of receiver or sender even though a message is encrypted. These types of attack are very difficult to track. But in active attack they change the operation of system .In the active attack there is alteration of the data by generating false data into the data stream. The active attack is divided into four types masquerade, modification, replay and denial of service.
In masquerade attack it pretends to be a person who is an attacker trying to send a message to the receiver

which thinks its from original source or sender.This is done by capturing the privileges own by sender for obtaining more privileges by masquerading it has the same privileges. The modification of the information is altered. This is delayed to generate wrong exchange of message. The attacker will change a small part of the information during this delay and send to the receiver. In the replay attack the capture of message from sender to receiver where later replay message to receiver side.denial of service where it will prevent from communication services. This is denial of a service in a network. They are done for performance degrading. This can be targeted to any of the services this can be mostly seen when offers are made by particular website selling during festive seasons or launching of product for flash sales.

The passive attacks which are difficult to trace in the ways it procure the essential data from large network. The information which is transmitted through the network is large. The attacker can analyze different information by the pattern of the information passed across the network. Side-channel attack is a passive attack where information is gathered from system without algorithm which is implemented in the system itself.

A timing attack watches the movement of the data in and out of data of the CPU or memory on the hardware running the cryptosystem or algorithm simply by observing variations in how it takes to perform cryptographic operations. It might be possible determine the secret key. Such attacks involve statically analysis of timing measurements and have been demonstrated across the networks. In order to increase the confidentiality and privacy of the image share an encryption algorithm is used. Digital knowledge can be understood in different ways. It can be text, video, audio etc.

Private video can be transmitted and can be used for storage purpose easily. But due to the growth of information age security and the issue in privacy is very important. An authorized can login to account for his private data which is very sensitive. The answer to above problem is by encrypting the video to protect from an unauthorized access. The traffic in network during video streaming which has a pattern develops a threat of privacy of user. The network have huge amount of traffic due to the amount of data people use is very huge. Variable bit rate encoding used for balancing the video bit rate

same. Video segments, its content and quality levels help the attacker to eavesdrop the traffic within a span of 3 minutes with a accuracy of 90 percent.. The quality level of video segment for playback, the pattern that is emerged helps for identification of videos. These mechanisms are seen in DASH which targets segment size variation of Variable bit rate and a particular traffic pattern. the identification of video in the traffic during video streaming without any change to video client and server. The differential bitrate based feature extraction for generating stable video features. The video finger prints and stream features are concatenated together for derive video identity by designing a partial matching method. The privacy of PC is challenged nowadays. There are two type of attacks passive an active attacks. The passive attack happens by eavesdrop of traffic from network side without direct contact with the device. The side-channel information of an encrypted traffic is used to collect the information about communications. This can be used for studying hugely for understanding the video streaming and web browsing etc. The research is mainly conducted on web traffic for its problems. Webpage can be monitored by the other people who can gain the personal information of user. It can be video information or text information mostly people prefer for storing theirinformation. So some webpages have to hide some information to get away from eavesdroppers. The side-channel attacks on encrypted data, mixed with the selective sections of web apps are becoming a threat for privacy of user data processed by applications which is highly confidential and sensitive. Side channel is cl assified

into two different categories of profiled and non-profiled where in profile phase a testing device which allows featuring the physical leakage and making an exact leakage model and non-profiled where attack is against a same target device to do a secret key extraction. Non-profile side channel attack includes differential power analysis, correlation power analysis variance ratio. Profile side channel attacks have stochastic approach and template attacks. Existing side channel attacks use an ideal measure environment with a mechanism to trigger the source code to get access to the target device. However this is not applicable to all real time events. Side channel data leakage in network studied vastly for more than a decade in the reference of cryptographic protocols and encrypted voice over internet protocol. Side-channel attacks have been there during the era of smart cards. Big Organizations wants strong security devices for analyzing the vulnerabilities in their networks. But with big scale networks and managing their complex configurations technically difficult. The network has to be changed with configuration change in other networks. The network admin wants to respond newly invented weakness by giving new patches and changes to the network configuration or utilizing resources to reduce the risk from attacks. The basic knowledge of visual secret sharing made for sharing visual information in the network. While other normal encryption or decryption processes, Visual secret sharing scheme has the advantage of make use of human visual system to decrypt the secret images without any complex mathematical computations. In this scheme, the encrypted image is split into m random shares. Then joining at least k shares to recover the original image. There is lot of research done in binary, grey-scale or color images. Since we used color and grey-scale image for hiding an information similar techniques are also used to hide image related to grey and color scale images. Most of the methods view on focusing to hide the information. Other than hiding, there is a method in which can restore the real image after reversing the hidden data for applications related to medical field and also geostrategic terrain images. These images must be highly secure and safe while sending to a specific person. Some uses a encryption method for securing the secret image with conventional encryption methods. The security depends whether the key generation algorithm is able to withstand a cryptanalysis or methods used to crack the key in possible ways. The image which is made into different shares using visual cryptography techniques and encrypting with a key is more secure.

III. VISUAL CRYPTOGRAPHY

Visual cryptography which was introduced by Shamir, Naor in 1995 is the technique based on human visual system. In this technique the encrypted data which is done by dividing the shares is decrypted by human eye. The complex structure of mathematical algorithms is not required in encryption and decryption. The images shares are encrypted into differentnumber of images. When the images are stacked together to match the sub pixels among the images. The implementation of this scheme is 2 shares. The shares uses exclusive xor operations .This scheme is extended into k out of n shares where less than k shares are needed .k<=n. Naor and Shamir used for only black and white images. After some years Verheaul and Tilborg developed a scheme for colored images. They use random shares to cover the secret images but the quality of images recovered is poor. When the cryptanalysis of the image shares are considered if attackers are able to gain all the shares only then recovering of original image share can be done.

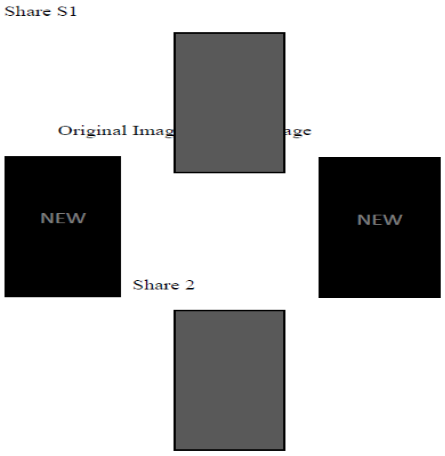


Fig.1: 2-out of 2 visual cryptography

In the above figure the representation of a secret image is made into shares in visual cryptography. The stacked image was obtained as a result of xoroperation .

Each pixel into a set of m black pixels white sub pixels in each of n shares for n-participants. When m=2 and n=2 its 2 out 2 scheme. To read all this images shares are stacked together. The result is reconstructed images of the secret image. But this image also contains noises. The display quality is affected by blackness and contrast value. Based on the degree of blackness there is deterministic model and probabilistic model. The (n,n)visual cryptographic schemes

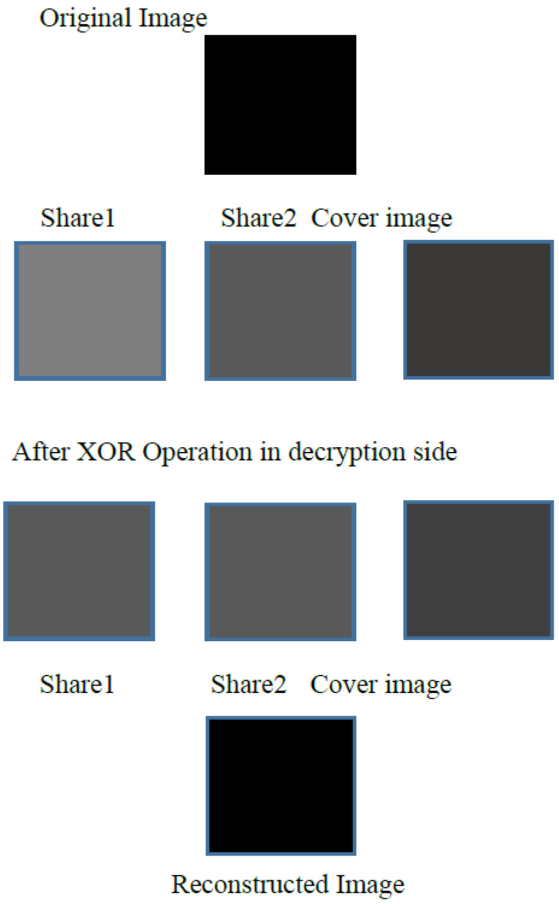


Fig.2 :k out of n visual cryptography

falls in first category and k,n visual cryptographic scheme in the later one. Researchers invented new visual cryptography techniques for gray scale and colored images. If The improvement of quality of images is limited in terms of development of VC algorithm where human eyes can perceive the image is not linked with the metrics used for quality measurement. There are researches where gray scale secret image is half toned by a quantizer of different level to generate binary images called halftone image and a threshold image. So different size invariant visual cryptography algorithms will be tested to the binary images these categories engulf the existing algorithms. In other category the intensity of block is quantized at various levels which turn represented by different patterns of binary images to accurate the local intensity. The secret images are encrypted into shares which can be considered as an analysis step for reconstructing the target image which is called synthesis step where image shares are binded .The target image in AbS process is pass on to analysis process where the pixel difference between target image and gray scale secret block is familiar to the encryption process.

Pixel	Probability	Stacking of shares	Pixels
White Pixel	0.5	■□□■	□ ■
	0.5	□■■□	■ □
Black pixels	0.5	□■■□	■
	0.5	■□□■	■

Fig.3: (2,2)scheme with 2 sub pixel stack

gray scale secret block is familiar to the encryption process. So the half toning method in encryption process can make changes to less the difference between the target image and secret block. i.e. the error between the original image and target image. Here in the above scheme m = 2 and n=2 so its called (2,2) scheme. The secret sharing expands the one pixel into several sub pixels. The recovered image is not the same exactly with the original one and makes it as noisy images.

When a pixel is black it choose two combinations. The two binded pixels become blacks. When binding white pixels in secret image are half-black and half white.The contrast of reconstructed image degraded by half percentage because degradation happened during the visual cryptography technique. The color images used by media are different. The contrast of pixels and the light colors usage. The gray level in images depends on the density of dark pixels. The way of using density of pixels needed is set to be scattered and those of dark areas are more and made gray level to half tone image. The human eye can see only concentrated region in the image.

Two models are used in color models. First additive model and subtractive models. In additive model Red, Green, Blue which is primary colors where colors are mixed to get composite colors. When all colors are mixed with equal wavelength (Red Green and Blue) obtain white color. Modulate the color Red, Green so we get different components of colors. The different colors which we get by mixing will add up the brightness of light. The compound color produces colors where more brightness is produced. The screen of computer is additive system. The other colors we see is combinations of primary colors. If we paint a wall with green color it will emit and blue color will absorb colors during natural sunlight.

While using computer the software's are of provided with image processing software's. The operating system are inbuilt itself with RGB color model. Here the screen of computer is output. The human retina identifies the RGB colors.

RGB color represents 0 to 255 color bits. Its 8 color bit each.

(0,0,0) represent black and (1,1,1) represent white. In Visual cryptography the using of shares we can makes the relationship between the complementary colors (Cyan, Magenta, Yellow) which are in the subtractive model. This visual cryptography can be identified using half

tone and grey color visual cryptography methods. The original image pixels and these are RGB pixel measures. Every pixel in the image is enhanced as shares. The shares of RGB image shares having RGB color components which are separated and also depend on the color image. The encryption of image is decided how much of shares are need to be generated.

The random grid based visual sharing scheme which help deal with general access structure and visual quality of reconstructed image .This paper proposes the security of proposed scheme and using generalized random visual secret sharing scheme quality of image in different situations. Analyzing the contrast of light in image in detail. They finally prove proposed method where optimal light contrast is minimal. The second part was proving the efficiency in the construction of the image without loss in quality. Here the image quality of reconstructed image are compared with Wu and Sun's scheme

In extended visual cryptography scheme a color images which was introduced by Droste. In a work for sharing a color images two extended visual cryptography was proposed. A 3 meaningful shares are proposed where it contains R,G ,B components of extended image. These three shares required for recovering original image and second method was two shares required for recover secret images. The components RG GB and RB contains secret image. The proposed method is made meaningful for increasing security where a cover image is also added with shares. The proposed technique in this paper is lossless in nature. The dimensions of cover images and of secret image and reconstructed images are same.

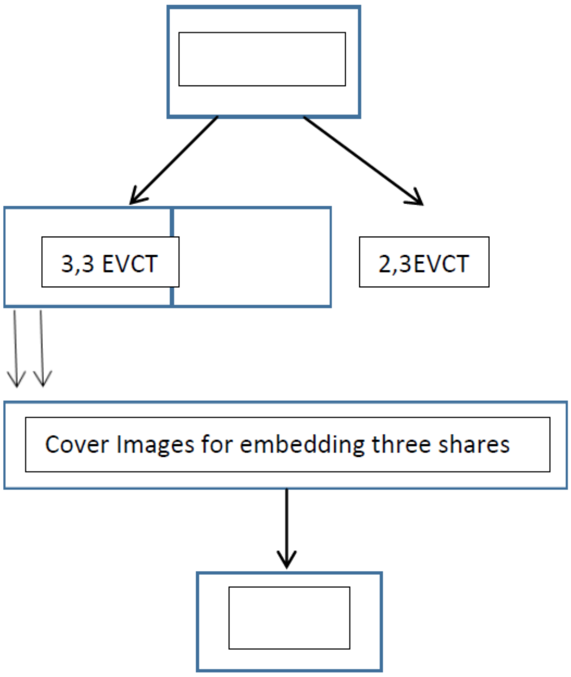


Fig.4: Extended Visual Cryptography for color images

The 3,3 EVCT and 2,3 EVCT are the two techniques to share color image. Here RGB image which is 24 bit made into 8-bit R G B components share using color decomposition. These are binded with the cover images to make them meaningful. These image shares are send to the communication medium. Every share contains 2 out of 3 components. RG, GB and RB share are created other than R, G,B shares. Hence 2,3 EVCT can produce original image. Error diffusion technique is used for high quality of visual data. The reconstructed images effectiveness are considered are on parameters such as total number of colors present in secret image. Operations performed on decryption side. Execution time for running the techniques and recovered images is lossy or not. The dimension of the image used in this experiment and applying the proposed techniques with high dimension images can also be analyzed. These techniques can be extended to general extended visual cryptography.

In chaos based visual cryptography the pixel position are used to generate the shares. This is done by using chaotic mapping where pixel values along with pixel positions are used.

In visual cryptography schemes sometimes fake shares can be inserted and remain a challenge. To avoid this XOR based visual cryptography schemewas proposed. To enhance the security these shares can be again encrypted by conventional encryption algorithms. These shares can be easily be retrieved at receiver side with fast execution and minimal peak signal noise ratio. Some visual cryptography watermarking technique is used for security. The public key cryptography like RSA algorithm is used for encrypting the image shares. This is for transmitting image shares more securely.

The progressive visual cryptography by stacking more image shares. The original image can be recovered only when more shares are binded together progressively. Here if we shadow images are binded together secret image cannot be identified which can be a security advantage in case of constructed threshold visual cryptography.

In multiple image visual cryptography, when image shares are produced in correlative matrices which is used to encode the binary secret images where each pixel corresponds to block and each block extended to form n x n pixels.

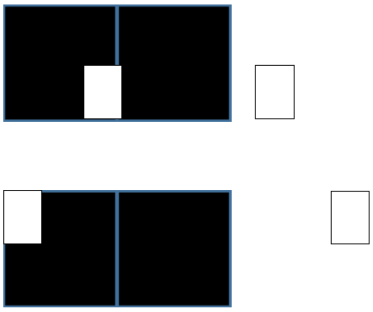


Fig.5:4 Different patterns of secret sharing

The extended block in the share will choose any of the patterns in the figure .This visual cryptography can hide more than one secret but contrast loss, security is issue. It have limits because here the image shares are square type the rotation angle is 0, 90,180, 270 only. Some changes in multiple secret sharing were done to overcome the limitation such as recursive visual cryptography. In recursive visual cryptography system images is made into shares and sub shares based on recursion. The security can be enhanced using recursion.

In the below tree representation of 2 out 2 visual cryptography system with recursion it involves two levels of encryption. S which is reconstructed by stacking shares in many ways

$$S = I1 + I2$$
$$S = I1 + I21 + I22$$
$$S = I2 + I11 + I12$$
$$S = I11 + I12 + I21 + I22$$

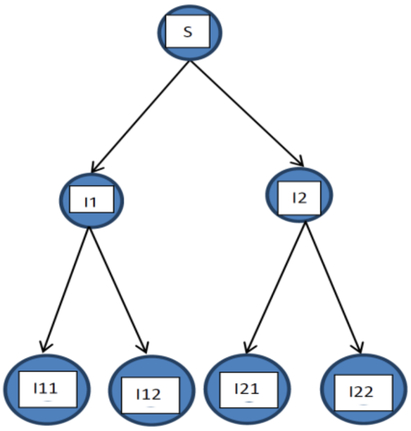


Fig.6:Two level of encryption for constructing Shares

The VCS using the many levels of encryption, the reliability and security can be improved. Here the first share is encrypted and second shares level is also again encrypted.

In segment based VC hiding message using numbers with seven segment display. The main importance in seven segment display the symbols are easily recognizable. The segment in seven segment display represented as Sn. The shares have no idea of hidden secret digit.

At the decryption side of visual cryptography the image shares are superimposed one with the other to recover the hidden secret image. There is XOR-based and OR-based VC. The shares which are produced based on OR-based VC where the pixel based which was used earlier. This is used because the reconstructed images are recovered from less number of shares. The quality of image is not degraded. Later when more shares started using the reconstructed image becomes darker. In XOR-based VC(Wu &Sun,2013) where the shares are superimposed to produce a good quality image. The XOR-based VC are commonly used logical operations at the receiver side.

Technique	No. of secrets	No. of shares	Pixel Expansion	Contrast loss	Computational Complexity
Bit-based VC	1	2	nil	1/2 or 1/4	-
Pixel-based VC	1	2	m	1/m	-
Extended VC	1	2	m	1/m	O(1)
Progressive VC	1	2	m	1/m	-
Multiple Image VC	2	2	m	1/m	O(1)
Segment based VC	1	n	nil	-	-
Chaotic VC	1	2	nil	-	-

Table 1: Different VC comparison based on parameters

The table represents the comparison between different visual cryptography. When the secret image reconstruction happens the black pixels in shares representing white pixels affect contrast loss. The size of shares used for generated by pixel based VC is directly proportional to the sub-pixels number in reconstructed image is termed as pixel expansion. The image reconstructed and having pixel expansion then size will be bigger for secret image which requires more storage space. The change in pixel intensity will affect the security. The time required for execution during the decryption must be small. So reducing the pixel expansion and contrast loss is important in visual cryptography. The strength of these techniques must be justified against histogram analysis, structural similarity index and bit error rate etc .Bit error rate is ratio between number of bit transmitted and received. Structural similarity index is the measure to find the alteration of structural information held by interdependent closed pixels and value lies between -1 to 1 .This helps about the objects in visual scene. Some of the images for transmission requires on the security aspect. The spatial image of region which have implications on security of a country. The threats can happen on both ways. The visual cryptography has various applications one is biometric privacy. The fingerprint and Iris are commonly used security feature for person. Visual cryptographic techniques are used to store and safe access into the official space and work.

In probabilistic VC the pixel expansion is focused which is arising from the pixel based VC. The contrast in the recovered secret image is same as that of pixel based. Each of the pixelsrepresent an image stored in computer as 1 bit number and common pixel format is the byte image where number stored as 8-bit ranging from 0 to 255.In intensity histogram pixel in the image at different intensity value. Some intrinsic characteristics of the image such as bulk data capacity and correlation in pixels traditional encryption like DES and IDEA not used. In flip-based visual cryptographic scheme two shares are encrypted into 2-dual based purpose shares where secret image is recovered from 2 transparencies. By flipping the one of 2 shares and binding with other share, second secret image is recovered. This scheme has optimal contrast and no pixel expansion.

Naor and Shamir proposed visual cryptography scheme. Initially the scheme was (2 ,2)-visual cryptography technique where 2-out-2 shares are reconstructed with the original image. The once which are shares are encrypted shares. The shares which are single cannot expose information in secret image. In each pixel can be expanded into many sub-pixels. It will have m sub-pixels after expansion.

The (k,n)-visual cryptography technique the color image and gray scale images by lattice based concept. The color images with C distinct colors shared using this technique. The (k,n) concept for color image have C subset in the finite lattice considered as pixels which corresponds to shares. The Naor and Shamir technique extended using linear programming for increasing the color contrast of the resultant images.

The improved security feature in extended visual cryptography by having the shares meaningful. The image shares are embedded by cover image to prevent the chaos created by something in secret image. The binary images where 2 white and 2 black sub pixel block and black pixel from cover images expanded to one white and three black sub pixels. When images are recovered block which correspond to black have 4 black sub pixels and block which points to white the final image as one white and three black pixels. The contrast lost by shares half the percent of image and recovered image by 75%.

The extended visual cryptography technique was improved by taking pixel from original image. These shares have 5 white and 7 black pixels of cover image accordingly. The block is 3x3 sub pixels in share images.

In gray scale images where Chang proposed the technique where size of the image shares does not change as per the color changes in image.

The proposed techniques where k,n visual cryptography technique for color and gray-scale images uses half-toning technique .These will reduce the contrast of the color image.

The threshold visual cryptography proposed by Chao and Lin using CMY color decomposition. The 24 bits true color original image is changed into 3 bit CMY halftone image. The 3 bit halftone image is made into 2 x 2 block which is based on concept of vectors. All pixels of 3 bits halftone C-M-Y images which are processed and the image shares are constructed. 2 out of 3 image shares construct the original image. The disadvantage of this technique is that resultant secret image is noisy and lossy in nature.

The other halftone visual cryptography proposed in where making m colored halftone image shares. The quality of image is high with less noise.

The k,n visual cryptography technique based on qualified subsets where any subset group G shares images with m persons share each a distinct secret. Its said that every subset is qualified. The constructed subset will have minimal pixel expansion and good contrast.

The proposed extended visual cryptography algorithm for 4 colored images as input and constructs any 3 images which are related to images given as input. During the stacking the 3 images are binded to get fourth image. The size is the same during decryption and the constructed image shares are meaningful.

Lou proposed a method in which visual cryptography can be used by using a watermark where this can be developed using a secret and public image. A certified authority registers with secret image. Using XOR operation the watermark is developed. The proposed (3,3) and (2,2)- extended visual cryptography for sharing secret images its extension of traditional visual cryptography. The gray-scale covers are embedded into them. The binding of shares reveals original image.

Shyong and Ming proposed integer linear programming for (k,n) VCS. The generalized visual cryptography system helps with minimal optimal expansion. In this a generalized integer linear programming constructs general visual cryptography visual system.

A (2,2) circular visual cryptography for binary images. The technique is that m secret image can be stored in circular plate at a time. Then shares are created. First share in small dimension and second share in bigger dimension (double) than first share. The first share is binded with share 1 of second secret image having dimensions bigger than first secret. Again the share 2 is constructed by combining 3rd image with first two images and the method continues until secret image are encapsulated in grid. This is turn into a circular plate until final shares are constructed. Decryption of image starts when largest dimensions is extracted firstly followed by the image which is half the dimension until the method is continued secret image is found out. As seen the explanation its clear about that the proposed algorithm can handle the images of various categories and images. The sizes of image also based in the encryption phase.

In the context of cryptography security in extended visual cryptography system the conflict by dissolving the multiple images to retrieve the original image from the given images This may spoil the result as a part of quantization error where the information from the sheet and target can interact with each other because of high frequency of conflict. But human high level visual system retains only ability to understand the image recovered from originals. This will become the schemenot secure. These can be addressed by experimenting on the contrast enhancement and analyzing the image quality resulting output images. The security based on the image where the trade-off between contrast enhancement and the security of the images. The extend to this scheme to color images where color images separated in channels of primary colors red,green,blue which can be treated as independent gray scale for each color channel.

In a very naive approach, the system applies the encryption to each channel and merges the result to get the colored output. Under the ideal subtractive color mixing model, stacking the two colored sheets reveals the colored target1. In reality, however, such ideal subtractive color mixture is unlikely due to the properties of ink, transparencies, etc. It needs to establish a sophisticated color mixing model for the extended visual cryptography with better color quality.

Visual cryptography helps to secure the shares of the image. Particle swarm optimization algorithm is one of the optimization algorithms which optimize the value in the complete solution space. The particle swarm optimization based on the size of cluster for knowledge sharing in solution. In local PSO the solution the position of particle in local cluster and differs from particle. In global iteration is performed for updating of position of particle. Each particle which is part of cluster are depicted as solution which is optimize solution for new group of particles. In a network every particle can be identified which can be a structure. In ring structure every adjacent particle which decides the speed of network for deciding new velocity. In cluster similar properties of particle are communicated by particle head and it acts the root of that cluster for the the individuals in that cluster. In a big network the particles which depict the best approach globally other than taking a local approach. The encryption side in visual cryptography for the shares. Other approach is differential evolution. The differential evolution genes decide the design in population It gives most relevant solution from a complete solution. In an image the primary colors like red green blue are chromosome. Here the new images are formed from the same image using existing images .Mutation in this images can helping generation of new image.

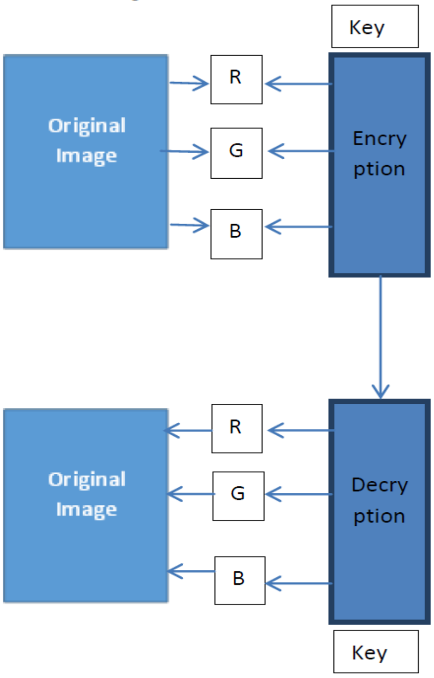
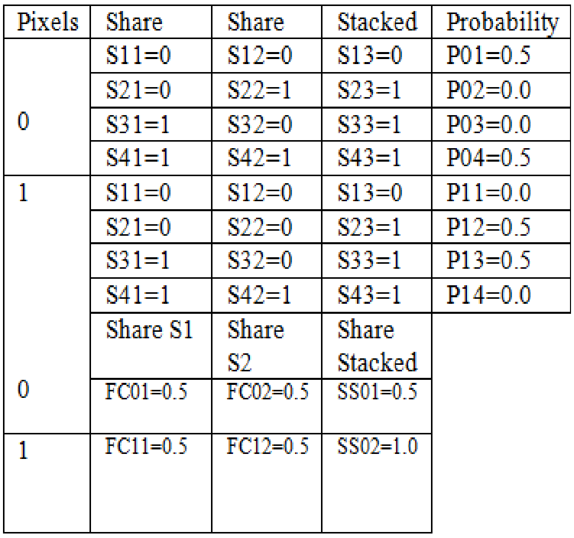


Fig.6: RGB shares secured transmission using a key

The original image which is spitted into three shares of RGB shares and encrypted. The encryption using a visual cryptography technique and a secret key generated by particle swarm optimization and encrypted by any cryptographic algorithm. The images are transmitted to the side of receiver. The key which is generated using optimization algorithm. In particle swarm optimization approach new images are formed where if differential evolution used for mutation of the particles. The values of color pixel are separated as RGB and the values from 0 to 255 are normalized. The encryption which is done by using best particle from resultant solution. The secret key obtained from final solution is used for encryption. The image shares are transmitted to receiver. The encrypted shares which constitute RGB colors are decrypted by the secret key and by superimposing all the image shares we get original image. Securing the sharing using the visual cryptography with the properties of conventional encryption of cryptography makes it harder to get the image which is divided and stored the match with a query. The original image is retrieved by superimposing the random images in regular manner. To decrease the time complexity multithread approach is used. The individual encryption of components in image (RGB) increases the encryption. In visual cryptography the security is a hard task. The pixel expansion reduction in pixel expanded techniques can be optimized and improved in some extent. The number of individuals increasing the expansion spike exponential. The storage space, the share transmission and the computation complexity as a result.

A genetic algorithm which was proposed by Holland in 1970.GAs is composed of chromosomes which represent a solution for a problem. A genetic algorithm uses solution for analyzing and best in the evaluation searching. The reproduction, crossover and mutation is the methods used by genetic algorithm. The reproduction method uses the chromosomes which is more durable is used in solution for genetic operations. The crossover used for exchanging the genes between two chromosomes to develop offspring. The mutation method for genetic alteration randomly. Therefore the genes which are suitable for present solution to the problem will happen in new solutions. The image half toning in region of binary image higher density because of the evenly distributed black pixels. The region becomes denser due to the degree of blackness. The probability of controlling the pixel in image help without a pixel expansion. The decryption process in visual cryptography where the human eyes can understand the difference in the black and white pixels from original image and superimposed image. If change in the rules of encryption it will make a difference in black and white spaces on the shares which are not identical



Pixels	Share	Share	Stacked	Probability
0	S11=0	S12=0	S13=0	P01=0.5
	S21=0	S22=1	S23=1	P02=0.0
	S31=1	S32=0	S33=1	P03=0.0
	S41=1	S42=1	S43=1	P04=0.5
1	S11=0	S12=0	S13=0	P11=0.0
	S21=0	S22=0	S23=1	P12=0.5
	S31=1	S32=0	S33=1	P13=0.5
	S41=1	S42=1	S43=1	P14=0.0
	Share S1	Share S2	Share Stacked	
0	FC01=0.5	FC02=0.5	SS01=0.5	
1	FC11=0.5	FC12=0.5	SS02=1.0	

Table 2: Probability for analyzing security and contrast

These tables are example for probability setting for good contrast and security. If changes are made in probability setting in the encryption of the image shares there will be a difference between black and white shares. The shares FC01=S11 x P01+S21 x P02 + S31 x P03 + S41 x P04 = 0.5 this shows the probability that a white pixel is encrypted as black pixel in S1 share. Here FC01=FC11=0.5 security is ensured.

The FC is the probability where white pixel is encrypted and binded as a black pixel on the stacked share of forbidden set.

The contrast of stacked probability that a white pixel encrypted and stacked as black pixel SS01 = S13 x P01 + S23 x P02 + S33 x P03 + S43 x P04 =0.5 and probability a black pixel is binded and encrypted as black pixel is 1.The main objective is to find the probability when contrast of stacked share is made optimized. Chromosomes are made of series of real numbers. The real parameter is used for avoiding the loss in precision by encoding method. Binary tournament selection method it picks two chromosomes with fitness values and chromosome with higher fitness value.

The visual cryptographic methods try to expand pixels and each share size become larger than original image. The distortion of shares also needs huge space. This will be leading to the difficulty in transmission of these shares and more requirements for storage. The probability concept was used for contrast issue for constructing an optimization model.

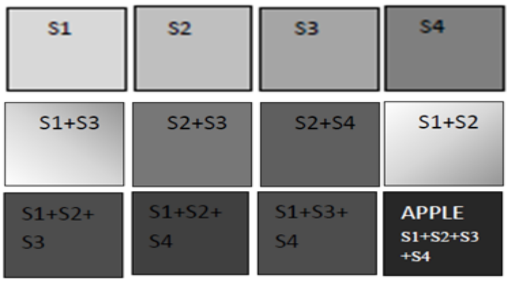


Fig.7: Probability concept for different stacked shares

From observing the above figure, It is much secure and it is easy to recognize the hidden information from the stacked shares. While using the probability model there is reconstruction of black pixels during the stacking. This is done in four shares of images. In the multiple images how much the probability model help to optimize and produce good results must be identified.

Images	Peak signal to Noise ratio	Mean squared error	Correlation co-efficient
Tree	53.00	1.23	0.9742
Jelly	36.38	0.385	0.9732
Lena	39.00	0.345	0.993
House	42.3	0.42	0.9782
Girl	55.00	0.20	0.9845

Table 3: Performance analysis of different standard test images

The table represents the performance in a system with attacks. This explains about the PSNR measure which is defined proportion of signals maximum availability to that of noise. Mean square error is average error in the occurrence in specific images. Correlation co-efficient which have two variables after encryption it will have higher correlation and identical when the correlation is 1 .This represents the hiding of information is failed .When the correlation coefficient is 0 it show major difference from the characteristics of original image.

In a digital watermarking method to get meaningful number of shares generated and also achieves more security. The water marking avoid active attack because it will not give idea about the original image. This method does not cause pixel expansion

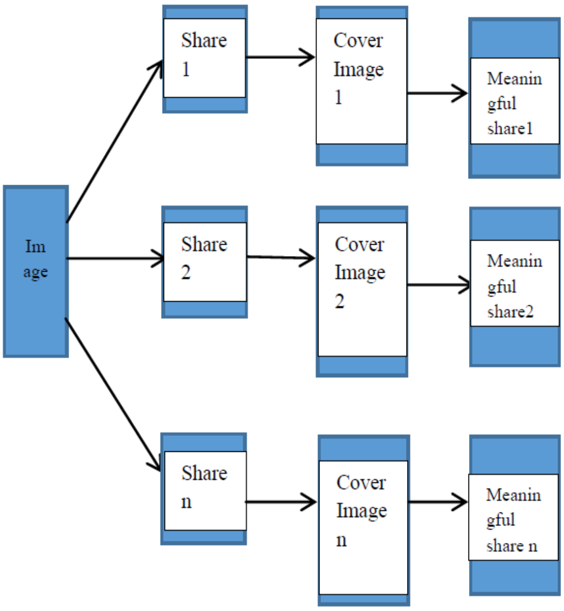


Fig.8: Securing multiple image shares using digital watermarking

The original image is tested with the watermarked image. The optimal number of shares decided based on the Structural similarity, Peak signal to noise ratio, Mean Squared error. Mean squared error is done to find if the two images are same. Peak signal ratio is test for signal strength.Sometimes a possible attack on a watermark image changes the behavior of image this is identified by robustness of the image. When an image is made into three colors by decomposition C,M,Y . The digital watermarking to shares avoids the identification about the original secret image.

In water marking algorithms the encoding of the source image or text is done using a secret key. This key is also used in the decoding side for gain the information source. The above figure represents the watermarking embedding scheme. A typical watermarking algorithm must have properties of capacity, imperceptibility and security. Capacity means the number of bits a watermarking algorithm can embed in source data.

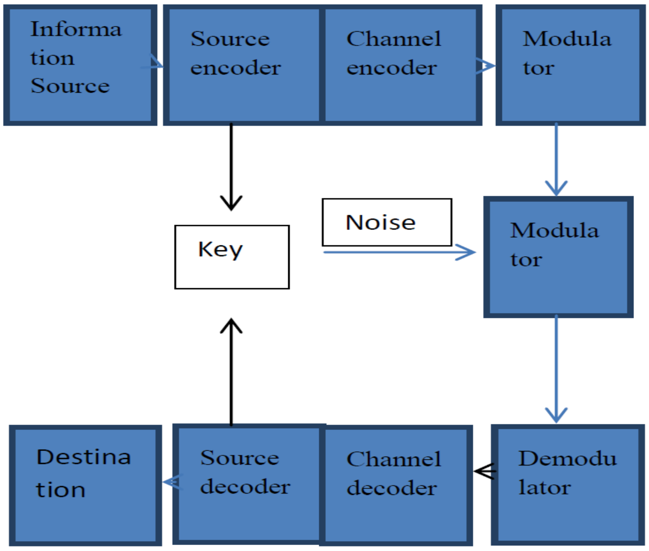
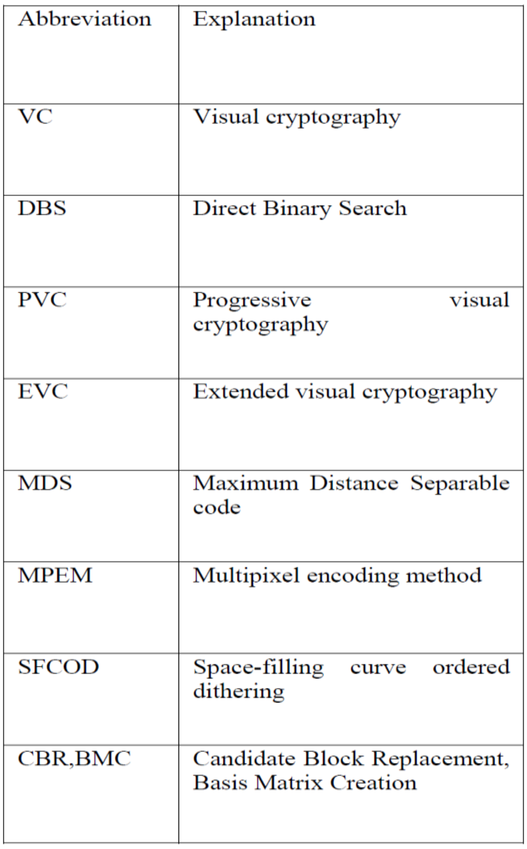


Fig.9 :Water marking encoding and decoding

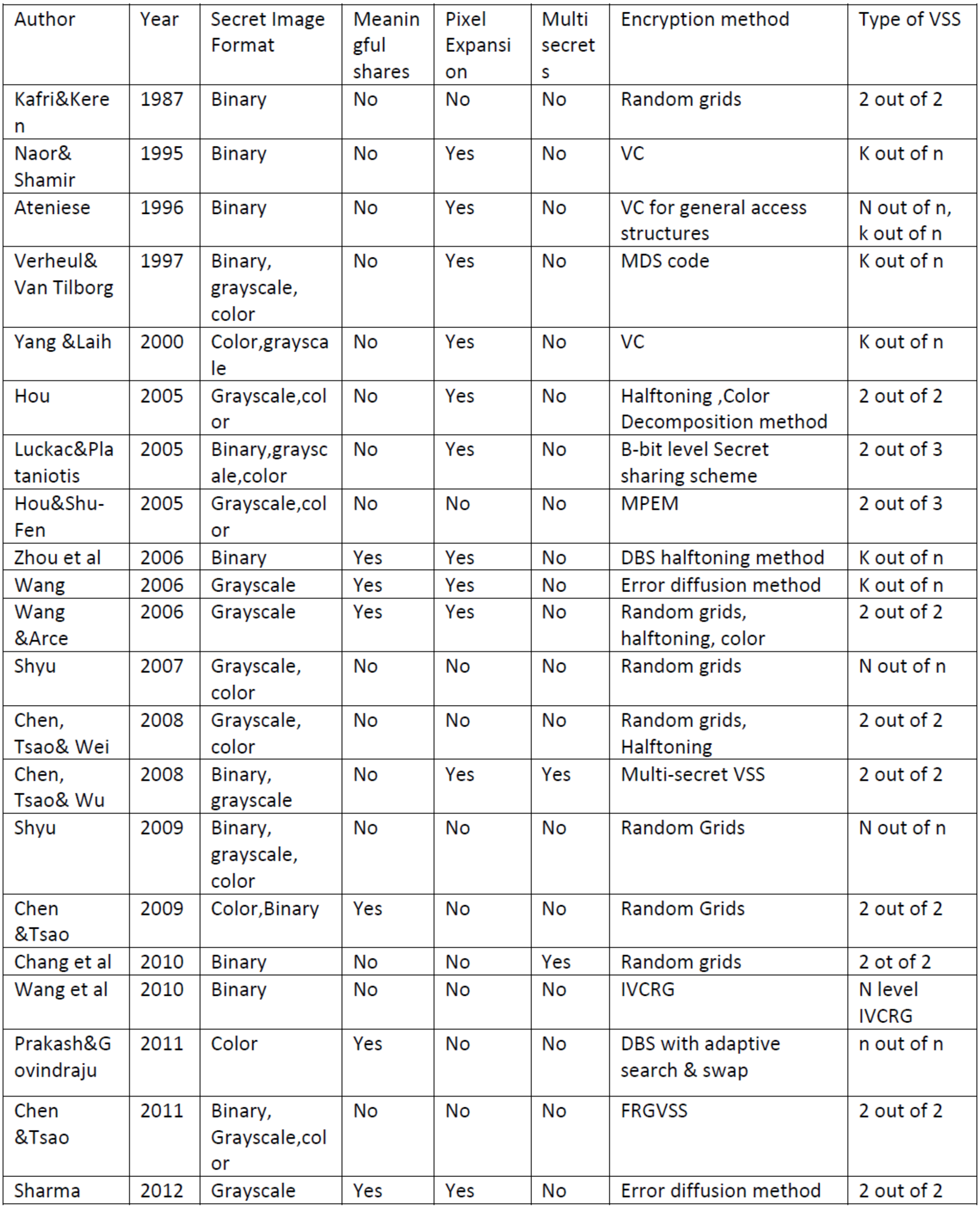
The security depends where the watermarking can help protecting the source data. The other property is robustness. This was about how watermark helps in preventing attacks. The robustness is important feature of watermarking. The digital watermarking ishaving three phases creation of watermark, encoding phase and decoding part for authentication. The meaningful shares that is generated for achieving the security. The watermarked shares will avoid the noise or hackers from getting the original secret. In visual cryptography multiple image secret sharing schemes watermarking system is used. In progressive visual cryptography for meaningful shares and unexpanded shares the watermarking methodology is used for security. The optimization algorithms involved in improving the performance and cost had helped to reduce the computation complexity involved in decryption side.

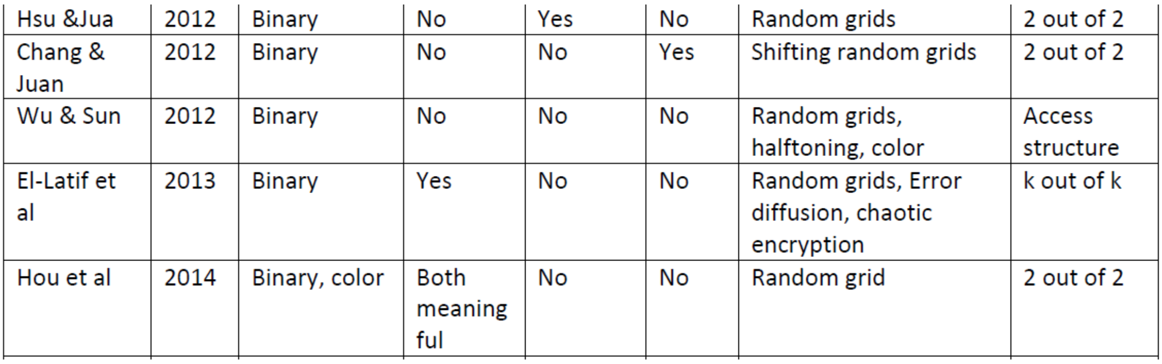
The evolution and improvement of different visual cryptography schemes is illustrated in table.



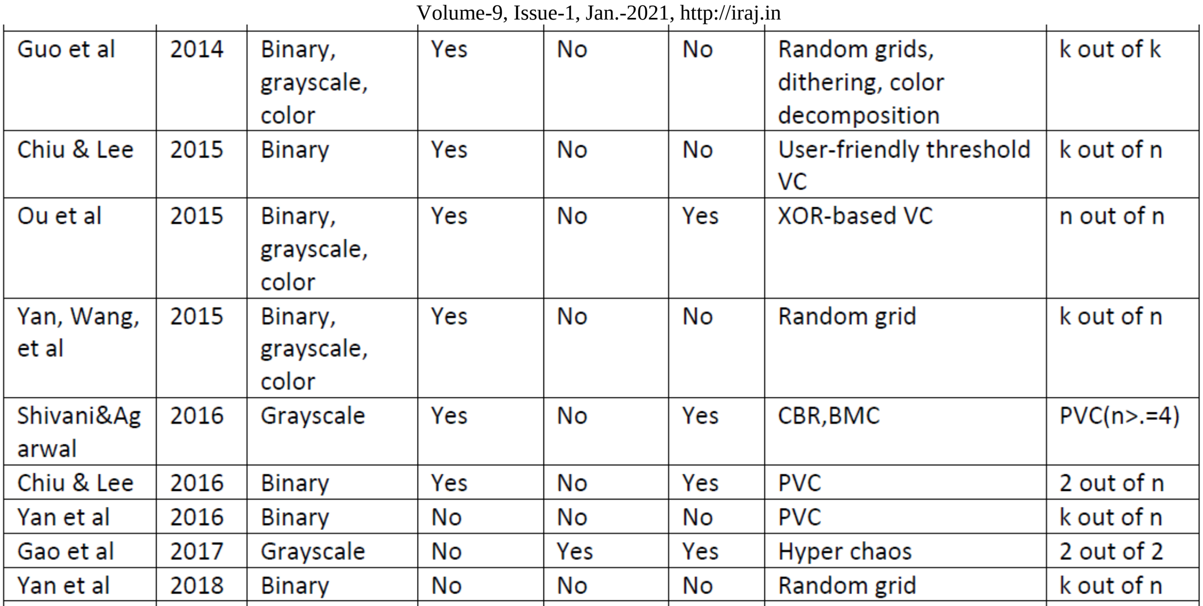
Abbreviation	Explanation
VC	Visual cryptography
DBS	Direct Binary Search
PVC	Progressive visual cryptography
EVC	Extended visual cryptography
MDS	Maximum Distance Separable code
MPEM	Multipixel encoding method
SFCOD	Space-filling curve ordered dithering
CBR,BMC	Candidate Block Replacement, Basis Matrix Creation

Table 4: Abbreviation used in Table 5





Author	Year	Secret Image Format	Meaningful shares	Pixel Expansion	Multi secrets	Encryption method	Type of VSS
Kafri&Keren	1987	Binary	No	No	No	Random grids	2 out of 2
Naor& Shamir	1995	Binary	No	Yes	No	VC	K out of n
Ateniese	1996	Binary	No	Yes	No	VC for general access structures	N out of n, k out of n
Verheul& Van Tilborg	1997	Binary, grayscale, color	No	Yes	No	MDS code	K out of n
Yang &Laih	2000	Color,grayscale	No	Yes	No	VC	K out of n
Hou	2005	Grayscale,color	No	Yes	No	Halftoning ,Color Decomposition method	2 out of 2
Luckac&Plataniotis	2005	Binary,grayscale,color	No	Yes	No	B-bit level Secret sharing scheme	2 out of 3
Hou&Shu-Fen	2005	Grayscale,color	No	No	No	MPEM	2 out of 3
Zhou et al	2006	Binary	Yes	Yes	No	DBS halftoning method	K out of n
Wang	2006	Grayscale	Yes	Yes	No	Error diffusion method	K out of n
Wang &Arce	2006	Grayscale	Yes	Yes	No	Random grids, halftoning, color	2 out of 2
Shyu	2007	Grayscale, color	No	No	No	Random grids	N out of n
Chen, Tsao& Wei	2008	Grayscale, color	No	No	No	Random grids, Halftoning	2 out of 2
Chen, Tsao& Wu	2008	Binary, grayscale	No	Yes	Yes	Multi-secret VSS	2 out of 2
Shyu	2009	Binary, grayscale, color	No	No	No	Random Grids	N out of n
Chen &Tsao	2009	Color,Binary	Yes	No	No	Random Grids	2 out of 2
Chang et al	2010	Binary	No	No	Yes	Random grids	2 ot of 2
Wang et al	2010	Binary	No	No	No	IVCRG	N level IVCRG
Prakash&Govindraju	2011	Color	Yes	No	No	DBS with adaptive search & swap	n out of n
Chen &Tsao	2011	Binary, Grayscale,color	No	No	No	FRGVSS	2 out of 2
Sharma	2012	Grayscale	Yes	Yes	No	Error diffusion method	2 out of 2
Hsu &Jua	2012	Binary	No	Yes	No	Random grids	2 out of 2
Chang & Juan	2012	Binary	No	No	Yes	Shifting random grids	2 out of 2
Wu & Sun	2012	Binary	No	No	No	Random grids, halftoning, color	Access structure
El-Latif et al	2013	Binary	Yes	No	No	Random grids, Error diffusion, chaotic encryption	k out of k
Hou et al	2014	Binary, color	Both meaningful	No	No	Random grid	2 out of 2



Guo et al	2014	Binary, grayscale, color	Yes	No	No	Random grids, dithering, color decomposition	k out of k
Chiu & Lee	2015	Binary	Yes	No	No	User-friendly threshold VC	k out of n
Ou et al	2015	Binary, grayscale, color	Yes	No	Yes	XOR-based VC	n out of n
Yan, Wang, et al	2015	Binary, grayscale, color	Yes	No	No	Random grid	k out of n
Shivani&Agarwal	2016	Grayscale	Yes	No	Yes	CBR,BMC	PVC(n>.=4)
Chiu & Lee	2016	Binary	Yes	No	Yes	PVC	2 out of n
Yan et al	2016	Binary	No	No	No	PVC	k out of n
Gao et al	2017	Grayscale	No	Yes	Yes	Hyper chaos	2 out of 2
Yan et al	2018	Binary	No	No	No	Random grid	k out of n

Hsu &Jua	2012	Binary	No	Yes	No	Random grids	2 out of 2
Chang & Juan	2012	Binary	No	No	Yes	Shifting random grids	2 out of 2
Wu & Sun	2012	Binary	No	No	No	Random grids, halftoning	Access structure
El-Latif et al	2013	Binary	Yes	No	No	Random grids, Error diffusion, chaotic encryption	k out of k
Hou et al	2014	Binary, color	Both meaningful	No	No	Random grid	2 out of 2
Guo et al	2014	Binary, grayscale, color	Yes	No	No	Random grids, dithering, color decomposition	k out of k
Chiu & Lee	2015	Binary	Yes	No	No	User-friendly threshold VC	k out of n
Ou et al	2015	Binary, grayscale, color	Yes	No	Yes	XOR-based VC	n out of n
Yan, Wang, et al	2015	Binary, grayscale, color	Yes	No	No	Random grid	k out of n
Shivani&Agarwal	2016	Grayscale	Yes	No	Yes	CBR,BMC	PVC(n>.=4)
Chiu & Lee	2016	Binary	Yes	No	Yes	PVC	2 out of n
Yan et al	2016	Binary	No	No	No	PVC	k out of n
Gao et al	2017	Grayscale	No	Yes	Yes	Hyper chaos	2 out of 2
Yan et al	2018	Binary	No	No	No	Random grid	k out of n

Table 5: Different type of visual cryptographic techniques

IV. CONCLUSION

In the network we discuss about the different type of attack. The attack which is very unable to trace is passive attack. This does not require any software or any algorithm for gaining the information. The amount of data especially multimedia data which is transmitted through network has a amount of loss due to the various factors which was discussed in this paper. This paper also discuss about visual cryptography. After analyzing from table there are more number of visual secret sharing schemes are being available and developed over the years. The amount of data that is transferred through network is huge. The concern for secure transmission of data is biggest challenge. The method to protect the multimedia data from unauthorized person is a threat for the distribution and major disadvantage for the business related to IT industry. The images that are used for encryption during the transmission require security with less decryption time. This will help for less computation complexity and also the cost of implementation of visual secret sharing scheme in a large network. There are many visual secret sharing schemes which is used for different purposes in real time environment. The visual cryptography techniques with different performance parameters are identified such as pixel expansion, quality of shares, size, visual quality recovered image, contrast, size of the image, computational complexity and number of shares generated for different visual cryptographic techniques.

REFERENCE

[1] Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R., " Visual cryptography for general access structures", Information and Computation, 129(2), 86–106. doi:10.1006/inco.1996.0076,1996

[2] Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R., "Extended capabilities for visual cryptography.", Theoretical Computer Science 250(1–2): 143–161. doi:10.1016/S0304-3975(99)00127-9,2001

[3] Chao, H. C., & Fan, T. Y., "XOR-based progressive visual secret sharing using generalized random grids", Displays, 49, 6–15. doi:10.1016/j.displa.2017.05.004, 2017

[4] Chen, T. H., &Tsao, K. H., "Visual secret sharing by random grids revisited", Pattern Recognition, 42(9), 2203–2217. doi:10.1016/j.patcog.2008.11.015

[5] Chen, T. H., &Tsao, K. H.," Threshold visual secret sharing by random grids ", Journal of Systems and Software, 84(7), 1197–1208. doi:10.1016/j.jss.2011.02.023,2011

[6] Chen, T. H., &Tsao, K. H., "User-friendly random-grid based visual secret sharing" , IEEE Transactions on Circuits and Systems for Video Technology, 21(11), 1693–1703. doi:10. 1109/TCSVT.2011.213347

[7] Chen, T. H., Tsao, K. H., & Lee, Y. S, "Yet another multiple-image encryption by rotating random grids", Signal Processing, 2012. doi:10.1016/j. sigpro.2012.02.015

[8] Chiu, P. L., & Lee, K. H., " User-friendly threshold visual cryptography with complementary cover images ", Signal Processing, 108, 476–488. doi:10.1016/j. sigpro.2014.09.032, 2015

[9] Chiu, P. L., & Lee, K. H., "An XOR-based progressive visual cryptography with meaningful shares", Computer Communication and the Internet (ICCCI), 2016 IEEE International Conference on (pp. 362–365), Wuhan, China: IEEE. doi:10.3389/fpls.2016.00362,2016

[10] Carlo Blundoa, StelvioCimatob, Alfredo De Santisa., "Visual cryptography schemes with optimal pixel expansion", Theoretical Computer Science 369 (2006) 169– 182, 2018

[11] El-Latif, A. A. A., Yan, X., Li, L., Wang, N., Peng, J. L., &Niu, X , " A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption ", Optics & Laser Technology, 54, 389–400. doi:10.1016/j. optlastec.2013.04.018,2013

[12] Hou, Y. C, "Visual cryptography for color images. Pattern Recognition, 36(7), 1619–1629. doi:10.1016/S0031-3203(02)00258-3,2003

[13] Ming Wang, Bo Cheng , and Chau Yuen, " Joint Coding-Transmission Optimization for a Video

[14] Surveillance System With Multiple Cameras",IEEE Transactions on multimedia, Vol. 20, No. 3, March 2018

[15] Venkata Krishna PavanKalubandi, HemanthVaddi, Vishnu Ramineni, AgilandeeswariLoganathan, "A Novel Image Encryption Algorithm using AES and Visual Cryptography ",IEEE 2nd International Conference on Next Generation Computing Technologies, 2016

[16] P.Geetha, Dr.V.S.Jayanthi, Dr. A.N. Jayanthi, "Optimal Visual Cryptographic Scheme with multiple share creation for

[17] Multimedia Applications", Computers & Security, Volume 78, 2018, Pages 301-320

[18] Ram Gopal Sharma, PritiDimri&HitendraGarg, "Visual cryptographic techniques for secret image sharing: a review", Information Security journal : A global perspective, https://doi.org/10.1080/19393555.2019.1567872,2019.

[19] JiaxiGu , Jiliang Wang, Zhiwen Yu , KeleShen, "Traffic-Based Side-Channel Attack in Video Streaming", IEEE/ACM Transactions on Networking,2018

[20] RinaldiMunir, Harlili, " Video Encryption by Using Visual Cryptography Based on Wang's Scheme", 4th International Conference on Electrical, Electronics and System Engineering,ICEESE,2018

[21] Nikhil C. Mhala, Rashid Jamal, Alwyn R. Pais, "Randomised visual secret sharing scheme for grey-scale and colour images", IET Image Processing, 2018

[22] Hussain M.J. Almohri, Layne T. Watson, Danfeng (Daphne) Yao, Xinming, "Security Optimization of Dynamic Networks with Probabilistic Graph Modeling and Linear Programming", IEEE Transactions on Dependable and Secure Computing, 2015

[23] RajatBhatnagar, Manoj Kumar," Visual Cryptography: A Literature Survey ", IEEE 2nd International conference on Electronics, Communication and Aerospace Technology ICECA,2018

[24] Xiaochun Cao, Na Liu, Ling Du, Chao Li, "Preserving privacy for video surveillance for visual cryptography", 978-1-4799-5403-2/14/$31.00 IEEE 2014

[25] Santos Merino Del Pozo, Francois-Xavier Standaert, Dina Kamel, Amir Moradi, "Side-Channel Attacks from Static Power:When Should we Care?", Automation & Test in Europe Conference & Exhibition (DATE),2015

[26] Pei-Ling Chiu and Kai-Hui Lee, "A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3,2011

[27] Pei-Ling Chiu, Kai-Hui Lee, "Optimization Based Adaptive Tagged Visual Cryptography", GECCO'18, July 15-19, 2018,

[28] Roberto De Prisco, Alfredo De Santis, "Color visual cryptography schemes for black and white secret images", Theoretical Computer Science ,2013

[29] Ran Dubinz, AmitDvir, OfirPeley, OferHadarz, "I Know What You Saw Last Minute -Encrypted HTTP Adaptive Video Streaming Title Classification, IEEE Transactions on Information Forensics and Security,2017

[30] AbulHasnat, Dibyendu Barman, Satyendra Nath Mandal , "A Novel Image Encryption Algorithm Using Pixel

[31] Shuffling and Pixel Intensity Reversal",IEEE International Conference on Emerging Technological Trends 2016

[32] Naoki Kita, Kazunori Miyata, "Magic sheets: Visual cryptography with common shares", Computational Visual Media Vol. 4, No. 2, 2018, 185–195

[33] AlIaLevina, DariaSleptsova, Oleg Zaitsev, "Side-Channel Attacks and Machine Learning Approach " 18TH Conference Of Fruct Association,2016

[34] KirtiDhiman, Singara Singh Kasana, "Extended visual cryptography techniques for true color images " , Computers and Electrical Engineering, https://doi.org/10.1016/j.compeleceng.2017.09.017,2017

[35] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition 36 , 1619 – 1629, 2002

[36] Imon Mukherjee, RitamGanguly, "Multiple video clips preservation using folded back audio-visual cryptography scheme", Springer Science+Business Media New York 2017

[37] Xiaokuan Zhang, Jihun Hamm, Michael K. Reitery, Yinqian Zhang, "Statistical Privacy for Streaming Traffic", Network and Distributed Systems Security (NDSS) Symposium, https://dx.doi.org/10.14722/ndss.2019.23210, 2019

[38] Ching-Sheng Hsu, Shu-Fen Tu, and Young-Chang Hou, "An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares" Springer-Verlag Berlin Heidelberg,2006

[39] Allan Pintoa, William Robson Schwartzb, HelioPedrinia, and Anderson Rocha, "Using Visual Rhythms for Detecting

[40] Video-based Facial Spoof Attacks", IEEE Transactions on Information Forensics And Security, 2015

[41] P. Punithavathi , S. Geetha Visual cryptography: A brief survey, Information Security Journal : A Global Perspective, 26:6, 305-317, DOI:10.1080/19393555.2017.1386249,2017

[42] Ming Tang, MaixingLuo, Junfeng Zhou, Zhen Yang, ZhipengGuo, Fei Yan, Liang Liu, Side-Channel Attacks in a Real Scenario", Tsinghua Science and Technology, 2018, 23(5): 586–598

[43] Raphael Spreitzer, VeelashaMoonsamy, Thomas Korak, Stefan Mangard, "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices, IEEE Communications Surveys and Tutorials,2017

[44] Shuo Chen, Rui Wang, XiaoFeng Wang, Kehuan Zhang, "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow", IEEE Symposium on Security and Privacy,2010

[45] Bin Yan, Yong Xiang, GuangHua," Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach, IEEE Transactions on Image Processing,2019

[46] Ching-NungYang,Dao-Shun Wang," Property Analysis of XOR-Based Visual Cryptography", IEEE Transactions On Circuits And System For Video Technology, VOL. 24, NO. 2,2014

[47] ZHAO Dongmeia,b, LIU Jinxing, "Study on Network Security Situation Awareness based on Particle Swarm Optimization Algorithm", Computers & Industrial Engineering , doi: https://doi.org/10.1016/j.cie., 2018

[48] Ross, A., & Othman A , " Visual cryptography for biometric privacy. IEEE Transactions on Information Forensics and Security, 2011

[49] Chettri L, GurungS,"Recursive information hiding in threshold visual cryptography scheme" International Journal of Emerging Technology and Advanced Engineering, 3(5):536–540, 2013

[50] Liu F, Wu C , " Embedded extended visual cryptography schemes", IEEE Transactions on Information Forensics and Security , 2011

[51] Lin SJ, Chung WH ,"A probabilistic model of (t,n) visual cryptography scheme with dynamic group." IEEE Transactions on Information Forensics and Security, doi: 10.1109/TIFS.2011.2167229,2012

[52] R. Gayathri, Dr. V. Nagarajan "Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme",IEEE ICCSP conference2015

[53] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., Aug. 2006.

[54] Wang, D. S, Zhang, L., Ma, N., et al. "Two secret sharing schemes based on Boolean operations", Pattern Recognition, 2007

[55] Yuanfeng Liu, Zhongmin "Halftone Visual Cryptography with Color Shares", IEEE International Conference on Granular Computing (GrC), 2012

[56] Liu, F., Wu, C. K., Lin, X, "Some extensions on threshold visual cryptography schemes". The Computer Journal,

[57] Wang D. S, Yi, F, "On converting secret sharing scheme to visual secret sharing scheme ", EURASIP Journal on

[58] F. Liu and C. Wu,"Embedded extended visual cryptography schemes", IEEE Transactions on Information. Forensics Security, 2011.

[59] K.-H. Lee, P.-L. Chiu, "Sharing visual secrets in single image random dot stereograms," IEEE Transactions on Image Processing, 2014.

[60] W. Ran-Zan, H. Shuo-Fang, "Tagged visual cryptography," Signal Processing Letters, IEEE, 2011

[61] M. Iwamoto, "A Weak Security Notion for Visual Secret Sharing Schemes",IEEE Transactions on Information Forensics and Security, 2012

[62] Munir, R, "Comparison of Secret Color Image Sharing Based on XOR Operation in RGB and YCbCr Color Space", Proceeding of ICEEI, 2017

[63] KulvinderKaur , VineetaKhemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption", Advance Computing Conference, Feb, 2013

[64] D.Wang, L. Dong, X. Li, "Towards Shift Tolerant Visual Secret Sharing Schemes", IEEE Transactions on Information Forensics and Security , 2011

[65] H. Abdolrahimpour, E. Shahab, "A Short Survey of Visual Cryptography and Secret Image Sharing Techniques and Applications", International Advanced Research Journal in Science, Engineering and Technology, 2017

[66] Shivani, S.: 'Vmvc: verifiable multi-tone visual cryptography', Multimedia Tools Appl., 2017, https://link.springer.com/article/10.1007/s11042-017-4422-6

[67] B. Shrivas, S. Yadav, "Visual Cryptography in the Video using Halftone Technique", International Journal of Computer Applications, 2015

[68] X.Wang, "Intelligent multi-camera video surveillance: A review," Pattern Recognition, Jan. 2013.

[69] D. S. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," Pattern Recognition, 2007.

[70] Yan, X., Wang, S., &Niu, X, "Threshold construction from specific cases in visual cryptography without the pixel expansion", Signal Processing, doi: 10.1016/j.

[71] sigpro.2014.06.011

[72] Sridhar, S, Sathishkumar R, Sudha, "Adaptive halftoned visual cryptography with improved quality and security", Multimedia Tools Appl.,2017

[73] Hou, Y. C., Wei, S. C., Lin, C. Y, "Random-grid based visual cryptography schemes. IEEE Transactions on Circuits and Systems for Video Technology", 2014

[74] doi:10.1109/TCSVT.2013.2280097

[75] M. Ulutas, G. Ulutas and V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme", The Journal of Systems and Software, 2011

[76] Weir, J.,Yan, W, "A comprehensive study of visua cryptography. In Transactions on data hiding and multimedia security ",Berlin, Heidelberg: Springer, 2010

[77] Yan, X., Wang, S., El-Latif A, Niu, X.,"Random grids-based visual secret sharing with improved visual quality via error diffusion", Multimedia Tools and Applications,2015.doi:10.1007/s11042-014-2080-5

[78] Roberto De Prisco, Alfred De Santis, "Color visual cryptography schemes for black and white secret images", Theoretical Computer Science , 2013

★★★